THE HONORABLE JOHN C. COUGHENOUR

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

STEVEN VANCE, *et al.*, Plaintiffs, v. MICROSOFT CORPORATION, Defendant.	No. 2:20-cv-01082-JCC-MAT DEFENDANT MICROSOFT CORPORATION'S MOTION TO DISMISS **NOTE ON MOTION CALENDAR**: OCTOBER 9, 2020 **ORAL ARGUMENT REQUESTED**

Davis Wright Tremaine LLP
LAW OFFICES
920 Fifth Avenue, Suite 3300
Seattle, WA 98104-1610
206.622.3150 main · 206.757.7700 fax

TABLE OF CONTENTS

Davis Wright Tremaine LLP
LAW OFFICES
920 Fifth Avenue, Suite 3300
Seattle, WA 98104-1610
206.622.3150 main · 206.757.7700 fax

TABLE OF AUTHORITIES

Page(s)

Cases

Davis Wright Tremaine LLP
LAW OFFICES
920 Fifth Avenue, Suite 3300
Seattle, WA 98104-1610
206.622.3150 main · 206.757.7700 fax

Davis Wright Tremaine LLP
LAW OFFICES
920 Fifth Avenue, Suite 3300
Seattle, WA 98104-1610
206.622.3150 main · 206.757.7700 fax

Statutes

Davis Wright Tremaine LLP
LAW OFFICES
920 Fifth Avenue, Suite 3300
Seattle, WA 98104-1610
206.622.3150 main · 206.757.7700 fax

Other Authorities

Davis Wright Tremaine LLP
LAW OFFICES
920 Fifth Avenue, Suite 3300
Seattle, WA 98104-1610
206.622.3150 main · 206.757.7700 fax

INTRODUCTION

Illinois residents Steven Vance and Tim Janecyk allege Microsoft violated the Illinois Biometric Information Privacy Act ("BIPA") when it downloaded an IBM-created dataset consisting of one million facial images, known as the Diversity in Faces Dataset ("DiF Dataset").[1] IBM allegedly created this dataset in 2019 "for the purpose of improving the ability of facial recognition systems to fairly and accurately identify all individuals." Dkt. 1, Complaint ("Compl.") ¶ 40. Plaintiffs seek to hold Microsoft liable for penalties under BIPA even though they allege IBM—not Microsoft—included their images and biometric information in the dataset.

Plaintiffs do so by alleging they voluntarily uploaded their photographs many years ago to Flickr, a photo-sharing website. They allege Flickr then made their images publicly available in a collection of 100 million photographs, from which IBM culled one million images to create the DiF Dataset. Plaintiffs do ***not*** allege Microsoft (i) interacted with them or any other Illinois Flickr users; (ii) conducted any activity relevant to this lawsuit in Illinois; (iii) ever linked Plaintiffs' identities with their individual biometric information; or (iv) ever engaged in any transactions to profit from Plaintiffs' data. They nevertheless contend BIPA governs Microsoft's out-of-state (i.e., Washington) conduct. And they assert Microsoft violated BIPA by "collecting and obtaining individuals' biometric identifiers and information ... without providing the requisite written information and without obtaining the requisite written releases." *Id.* ¶ 94. They seek to bring these claims on behalf of a class of any other Illinois residents whose images appear in the IBM DiF Dataset.

---

[1] Plaintiffs Vance and Janecyk, represented by the same counsel, are pursuing a substantially identical putative class action against Amazon, claiming BIPA violations based on allegations that, like Microsoft, Amazon downloaded the DiF Dataset from IBM. *See Vance et al. v. Amazon.com, Inc.*, W.D. Wash. No. 2:20-cv-01084-RAJ. Microsoft understands Amazon is likewise filing a motion to dismiss the claims against it, asserting the same dismissal arguments Microsoft asserts in this motion.

Davis Wright Tremaine LLP
LAW OFFICES
920 Fifth Avenue, Suite 3300
Seattle, WA 98104-1610
206.622.3150 main · 206.757.7700 fax

Plaintiffs fail to state a claim, and the Court should dismiss the Complaint with prejudice under Rule 12(b)(6), for the following reasons:

First, the BIPA claims (Counts I and II) fail because BIPA does not express clear intent to apply extraterritorially, as required for Illinois statutes to have such effect. Thus, the statute could regulate Microsoft only if its BIPA-related conduct occurred primarily and substantially in Illinois. But Plaintiffs fail to allege Microsoft engaged in ***any*** conduct in Illinois giving rise to BIPA liability. Plaintiffs allege only that the IBM DiF Dataset, which Microsoft allegedly downloaded, included publicly-available online photographs of Vance and Janecyk, and that Microsoft conducts business in Illinois related to facial-recognition technology more generally. This is plainly insufficient. BIPA does not reach Microsoft's alleged conduct.

Second, applying BIPA to Microsoft's out-of-state conduct would violate the dormant Commerce Clause, which "precludes the application of a state statute" that has "the practical effect of ... control[ling] conduct beyond the boundaries of the State," "whether or not the commerce has effects within the State." *Healy v. Beer Inst., Inc.*, 491 U.S. 324, 336 (1989). If Plaintiffs could state a BIPA claim against Microsoft, that would mean a business in Washington could not engage in an online transaction with a business in New York without subjecting itself to penalties in Illinois—even if the Washington business does nothing in Illinois relating to the transaction and the transaction complies with Washington law. The dormant Commerce Clause bars such an outcome.

Third, even if BIPA applied (and it should not), Plaintiffs fail to state a claim under its plain language. Neither Section 15(b) nor Section 15(c) of BIPA applies to biometric information derived from "photographs." Section 15(b) also does not afford an action for mere passive possession of biometric identifiers or information. And Plaintiffs fail to plausibly plead that Microsoft "profited" from their biometric identifiers or information and thus fail to state a Section 15(c) claim.

Davis Wright Tremaine LLP
LAW OFFICES
920 Fifth Avenue, Suite 3300
Seattle, WA 98104-1610
206.622.3150 main · 206.757.7700 fax

Fourth, Plaintiffs fail to state an unjust enrichment claim (Count III) because they do not plausibly allege (i) Microsoft was enriched by their biometric identifiers or biometric information; (ii) they suffered any expense or loss; or (iii) they lack an adequate remedy at law, given the alleged BIPA violation serves as the only basis for the unjust enrichment claim.

Fifth, Plaintiffs' "injunctive relief" claim (Count IV) amounts to nothing more than a prayer for relief, not a claim, and should therefore be dismissed.

FACTUAL BACKGROUND

A. The Illinois Biometric Information Privacy Act.

The Illinois General Assembly enacted BIPA in 2008 to address the growing use of biometric technology "in the business and security screening sectors" in Illinois. 740 ILCS 14/5(a). The General Assembly found "[m]ajor national corporations ha[d] selected the City of Chicago and other locations in [Illinois] as pilot testing sites for new applications of biometric-facilitated financial transactions, including finger-scan technologies at grocery stores, gas stations, and school cafeterias." 740 ILCS 14/5(b). The Illinois legislature also found that consumers had concerns about "use of biometrics when such information is tied to finances" and were "deterred from partaking in biometric identifier-facilitated transactions," in part because of the "limited State law regulating the collection, use, safeguarding, and storage of biometrics." 740 ILCS 14/5(d), (e).

BIPA addresses these concerns by regulating the collection, possession, and storage of certain biometric identifiers and information, while expressly excluding coverage of other data. The statute defines "biometric identifier" using a short, exclusive list of personal data: "'[b]iometric identifier' means a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry." 740 ILCS 14/10. Section 15(b) requires private entities that "collect, capture, purchase, receive through trade, or otherwise obtain a person's ... biometric identifier or biometric information" to first (1) inform the person of that collection "in writing"; (2) inform the person "in writing of the specific purpose and length of term" regarding the

Davis Wright Tremaine LLP
LAW OFFICES
920 Fifth Avenue, Suite 3300
Seattle, WA 98104-1610
206.622.3150 main · 206.757.7700 fax

collection; and (3) obtain a "written release" from the person. 740 ILCS 14/15(b). Section 15(c) further prohibits any private entity "in possession of a biometric identifier or biometric information" from "sell[ing], leas[ing], trad[ing], or otherwise profit[ing] from a person's ... biometric identifier or biometric information." 740 ILCS 14/15(c).

For negligent violations of BIPA, a plaintiff may obtain "liquidated damages of $1,000 or actual damages, whichever is greater," and for intentional or reckless violations of BIPA, a plaintiff may collect "liquidated damages of $5,000 or actual damages, whichever is greater." 740 ILCS 14/20(2).

B. The IBM DiF Dataset.

Plaintiffs Vance and Janecyk allege that, in 2008 and 2011, respectively, they uploaded photos of themselves to the photo-sharing website Flickr. Compl. ¶¶ 60, 69. Each alleges he uploaded his photos using a device in Illinois. *Id.*

Plaintiffs contend that, in 2014, Yahoo!—Flickr's parent company at the time—released to the public approximately 100 million photos uploaded by Flickr users (the "Flickr Dataset"). *Id.* ¶ 29. Oath Inc.—the current name of the entity formerly known as Yahoo!—is a Delaware corporation headquartered in Sunnyvale, California.[2] Plaintiffs do not allege any interaction or relationship between Flickr and Microsoft.

Plaintiffs next assert IBM in 2019 created the DiF Dataset "consisting of one million images culled from the Flickr Dataset ... for the purpose of improving the ability of facial recognition systems to fairly and accurately identify all individuals." *Id.* ¶ 40. Plaintiffs

---

[2] *See* State of Delaware, *Department of State: Division of Corporations, Business Search Results for Oath Inc.*, https://icis.corp.delaware.gov/ecorp/entitysearch/NameSearch.aspx (last accessed Sept. 10, 2020). The Court may take judicial notice of information posted on a state government website because it is "readily verifiable and, therefore, the proper subject of judicial notice." *Reyn's Pasta Bella, LLC v. Visa USA, Inc.*, 442 F.3d 741, 746, n.6 (9th Cir. 2006); *see also L'Garde, Inc. v. Raytheon Space & Airborne Sys.*, 805 F. Supp. 2d 932, 938 (C.D. Cal. 2011) (taking judicial notice of "Business Entity Detail" search result from Secretary of State website submitted in support of motion to dismiss).

Davis Wright Tremaine LLP
LAW OFFICES
920 Fifth Avenue, Suite 3300
Seattle, WA 98104-1610
206.622.3150 main · 206.757.7700 fax

contend IBM included their publicly available Flickr photos in the DiF Dataset, and in creating the dataset, IBM "scanned the facial geometry of each image contained in the dataset" and created "biometric identifiers" and "biometric information" from the photographs. *Id.* ¶ 41. According to Plaintiffs, the IBM DiF Dataset included a "'comprehensive set of annotations of intrinsic facial features that includes craniofacial distances, areas and ratios, facial symmetry and contrast, skin color, age and gender predictions, subjective annotations, and pose and resolution.'" *See id.* ¶¶ 39–41.

IBM is a New York corporation with its headquarters in New York, New York.[3] Plaintiffs do not allege IBM created the DiF Dataset in Illinois, or even that IBM knew the culled images included photographs of Illinois residents. Nevertheless, they allege BIPA regulates the purported "biometric identifiers" and "biometric information" IBM allegedly created from the Flickr photographs. *Id.* ¶¶ 41–44. Plaintiffs further allege IBM made the DiF Dataset available to other companies. *Id.* ¶¶ 44, 47.

C. Microsoft's Alleged Conduct.

Plaintiffs assert Microsoft "applied for and obtained the Diversity in Faces Dataset from IBM." *Id.* ¶ 55. Plaintiffs do ***not*** plead facts showing Microsoft's alleged acquisition of the IBM DiF Dataset had any connection whatsoever with Illinois. Plaintiffs do not claim they personally uploaded photos to Microsoft servers, used Microsoft software, services, or technology, or ever communicated or interacted with Microsoft. Nor do Plaintiffs allege any of Microsoft's actions in purported violation of BIPA—e.g., "collecting, capturing and otherwise obtaining the[ir] biometric identifiers and information" and/or "profit[ing]" from that data, *id.* ¶¶ 58, 65–66, 73–74, 101—occurred in Illinois. Microsoft's only alleged connections to Illinois are: (1) allegedly possessing IBM's DiF Dataset of publicly-available

---

[3] *See* New York State, *Department of State, Division of Corporations, State Records & UCC, Search The Corporation and Business Entity Database Results for International Business Machines Corporation*, https://www.dos.ny.gov/corps/bus_entity_search.html (last accessed Sept. 10, 2020).

Davis Wright Tremaine LLP
LAW OFFICES
920 Fifth Avenue, Suite 3300
Seattle, WA 98104-1610
206.622.3150 main · 206.757.7700 fax

photos of approximately one million individuals, some undetermined number of which purportedly include Illinois residents, *id.* ¶¶ 63, 71; and (2) allegedly conducting "extensive business within Illinois related to the facial recognition products it unlawfully developed"—in some unspecified way—"using Plaintiffs' ... biometric identifiers and information." *Id.* ¶ 59.

ARGUMENT

Rule 12(b)(6) requires dismissal when a plaintiff "fail[s] to state a claim upon which relief can be granted." Fed. R. Civ. P. 12(b)(6). To plead a viable cause of action, the allegations must transcend the "speculative," "conceivable," and "possible," and must "state a claim that is plausible on its face." *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555–57, 566–67, 570 (2007). The Court must disregard "legal conclusions" and "conclusory statements," and scrutinize factual allegations to ensure they are more than "merely consistent with a defendant's liability." *Ashcroft v. Iqbal*, 556 U.S. 662, 677–79 (2009).

I. THE COURT SHOULD DISMISS PLAINTIFFS' BIPA CLAIMS.

The Court should dismiss Plaintiffs' BIPA claims because the claims violate Illinois's extraterritoriality doctrine and the dormant Commerce Clause, and fail to state a claim under BIPA's plain language.

A. BIPA Does Not Apply Extraterritorially to Microsoft's Alleged Conduct.

Under Illinois law, "a statute is without extraterritorial effect unless a clear intent in this respect appears from the express provisions of the statute." *Avery v. State Farm Mut. Auto. Ins. Co.*, 835 N.E.2d 801, 852 (Ill. 2005) (citation omitted). "[N]one of BIPA's express provisions indicates that the statute was intended to have extraterritorial effect." *Monroy v. Shutterfly, Inc.*, 2017 WL 4099846, at *5 (N.D. Ill. Sept. 15, 2017). Because BIPA "was not intended to and does not have extraterritorial application," "asserted violations of [BIPA] must have taken place in Illinois" to fall within the statute. *Rivera v. Google, Inc.*, 238 F. Supp. 3d 1088, 1100, 1104 (N.D. Ill. 2017). The statute requires an assessment "as to where the essential elements of a BIPA violation take place." *Patel v. Facebook, Inc.*, 932 F.3d

Davis Wright Tremaine LLP
LAW OFFICES
920 Fifth Avenue, Suite 3300
Seattle, WA 98104-1610
206.622.3150 main · 206.757.7700 fax

1264, 1276 (9th Cir. 2019).

Microsoft thus could be subject to BIPA only if "the majority of circumstances relating to the alleged violation of the [statute]" occurred in Illinois. *Landau v. CNA Fin. Corp.*, 886 N.E.2d 405, 409 (Ill. App. 2008). Put another way, for BIPA to apply to Microsoft, "the circumstances relating to the claim [must have] occur[ed] primarily and substantially" in Illinois. *Avery*, 835 N.E.2d at 853; *see also Patel*, 932 F.3d at 1275–76 (applying "primarily and substantially" test to BIPA claim). Plaintiffs' claims fail this test.

The primary and substantial elements of the Section 15(b) claim would involve Microsoft's alleged "collection" of Plaintiffs' biometric data from IBM without prior notice to them and without their written consent. *See* Compl. ¶ 94; 740 ILCS 14/15(b). The elements of Plaintiffs' Section 15(c) claim would involve Microsoft's alleged "profit[ing]" from their biometric data. *See* Compl. ¶ 101; 740 ILCS 14/15(c). But Plaintiffs do not allege Microsoft engaged in any of this conduct in Illinois—and they could not so allege consistent with their obligations under Rule 11. Fed. R. Civ. P. 11.

Microsoft's alleged possession of photographs of Illinois residents, Compl. ¶¶ 63, 71, even if true, would ***not*** show it collected biometric information or profited from that information in Illinois. On the contrary, Plaintiffs allege Microsoft obtained the DiF Dataset online from IBM, a New York corporation, for free. Compl. ¶¶ 49, 55, 56. And Plaintiffs fail to allege this non-commercial transaction occurred "primarily and substantially" in Illinois—something, again, they would have no good faith basis to allege.

Plaintiffs also allege Microsoft "(i) sell[s] its facial recognition products to third-party clients through an Illinois-based vendor; (ii) work[s] closely with an Illinois-based business to build new applications for its facial recognition technology; and (iii) work[s] with the University of Illinois, among others, to build and promote a 'digital transformation institute' aimed at 'accelerating the application of artificial intelligence' throughout business and society." Compl. ¶ 59. But Plaintiffs' conclusory allegations do not plausibly explain how

Davis Wright Tremaine LLP
LAW OFFICES
920 Fifth Avenue, Suite 3300
Seattle, WA 98104-1610
206.622.3150 main · 206.757.7700 fax

these activities have any connection to the IBM DiF Dataset. In particular, Plaintiffs fail to allege the DiF Dataset, released in 2019, played any role in Microsoft's development of any facial-recognition technology purportedly licensed or sold in Illinois—let alone photographs ***from Illinois residents*** specifically were used in that development.

In alleging Microsoft "work[ed] with the University of Illinois, among others, to build and promote a 'digital transformation institute' aimed at 'accelerating the application of artificial intelligence' throughout business and society," *id.*, Plaintiffs quote (without citation) a March 2020 article from the Microsoft News Center. *See C3.ai, Microsoft, and leading universities launch C3.ai Digital Transformation Institute* (Mar. 26, 2020), Microsoft News Center, https://news.microsoft.com/2020/03/26/c3-ai-microsoft-and-leading-universities-launch-c3-ai-digital-transformation-institute/ (last accessed September 11, 2020). But the "artificial intelligence" discussed in the article has ***nothing*** to do with facial-recognition technology; rather, it involves the use of AI to mitigate COVID-19's spread. *See id*. (Because Plaintiffs quote this article, the Court may consider it on this motion. *See Daniels-Hall*, 629 F.3d at 998–99 (considering documents referenced in complaint in ruling on motion to dismiss).) Plaintiffs have alleged no plausible connection between Illinois and Microsoft's alleged download of the IBM DiF Dataset.

The few cases that have found it premature to determine at the motion to dismiss stage whether a plaintiff's claims would require an extraterritorial application of BIPA do not apply here. In particular, in each of those cases an Illinois plaintiff allegedly uploaded a photo ***directly*** to the ***defendant's*** systems from a computer or device located in Illinois, so the defendant's collection arguably occurred in Illinois. *See, e.g.*, *Patel*, 932 F.3d at 1268, 1276 (Illinois-based Facebook users uploaded their photos to Facebook from Illinois); *Monroy*, 2017 WL 4099846, at *6 (plaintiff "allege[d] that [his] photo was uploaded to Shutterfly's website from a device that was physically located in Illinois and had been assigned an Illinois-based IP address"); *Rivera*, 238 F. Supp. 3d at 1101 (plaintiff's "photographs were allegedly

Davis Wright Tremaine LLP
LAW OFFICES
920 Fifth Avenue, Suite 3300
Seattle, WA 98104-1610
206.622.3150 main · 206.757.7700 fax

'automatically uploaded in Illinois to [Google's] cloud-based Google Photos service . . . from an Illinois-based Internet Protocol ('IP') address'" (citation omitted)). Here, by contrast, Plaintiffs allege they uploaded their photos from their devices in Illinois directly to ***Flickr***; they do not allege they uploaded ***anything*** to Microsoft (or even IBM), much less that they did so in Illinois. Indeed, Plaintiffs do not allege they ever interacted with Microsoft at all—in Illinois or anywhere else—or that Microsoft had any interactions in Illinois showing supposed collection, use, or profit from the IBM DiF Dataset.

In short, the Complaint does not allege Microsoft's purported conduct occurred "primarily and substantially" in Illinois, as required to state a claim under Illinois law. *Avery*, 835 N.E.2d at 853; *see also Neals v. PAR Tech. Corp.*, 419 F. Supp. 3d 1088, 1091–92 (N.D. Ill. 2019) (dismissing BIPA complaint with leave to amend where court was "unable to reasonably infer from the complaint that [plaintiff's] fingerprint was collected in Illinois"); *Tarzian v. Kraft Heinz Foods Co.*, 2019 WL 5064732, at *3 (N.D. Ill. Oct. 9, 2019) (dismissing Illinois consumer fraud claims under Rule 12(b)(6) based on absence of Illinois connection). The Complaint therefore fails to state a claim against Microsoft under BIPA.

B. Plaintiffs' BIPA Claims Violate the Dormant Commerce Clause.

1. Plaintiffs' Claims Impermissibly Attempt to Regulate Conduct Occurring Entirely Outside Illinois's Borders.

Similar to Illinois's extraterritoriality doctrine, the U.S. Constitution ensures a state regulates only the conduct that that state has a substantial interest in controlling. Article I, section 8 gives Congress the exclusive power to regulate commerce "among the several states." This express grant of power implicitly "limit[s] ... the authority of the States to enact legislation affecting interstate commerce" and "precludes the application of a state statute" that has "the practical effect of ... control[ling] conduct beyond the boundaries of the State ... whether or not the commerce has effects within the State." *Healy*, 491 U.S. at 336 n.1.

Davis Wright Tremaine LLP
LAW OFFICES
920 Fifth Avenue, Suite 3300
Seattle, WA 98104-1610
206.622.3150 main · 206.757.7700 fax

"[T]he dormant Commerce Clause . . . has at least two emanations": (1) when a state statute "discriminates against interstate commerce, or when its effect is to favor in-state economic interests over out-of-state interests"; and (2) "direct regulation emanation"—i.e., "when a state law directly affects transactions that take place across state lines or entirely outside of the state's borders." *Daniels Sharpsmart, Inc. v. Smith*, 889 F.3d 608, 614–15 (9th Cir. 2018) (quoting *S.D. Myers, Inc. v. City & County of San Francisco*, 253 F.3d 461, 467 (9th Cir. 2001)). If a state statute directly regulates conduct "wholly outside of the state's borders," the statute is "struck down ... without further inquiry." *Chinatown Neighborhood Ass'n v. Harris*, 794 F.3d 1136, 1145–46 (9th Cir. 2015) (citation omitted).

Because Plaintiffs do not allege Microsoft engaged in ***any*** relevant conduct in Illinois, the "practical effect" of Plaintiffs' BIPA claims would be to allow Illinois to control conduct entirely beyond its boundaries. Plaintiffs' claims therefore violate the "direct regulation" emanation of the dormant Commerce Clause. *See, e.g.*, *Daniels Sharpsmart, Inc.*, 889 F.3d at 614–15 (California Medical Waste Management Act likely violated dormant Commerce Clause by "attempt[ing] to reach beyond the borders of California [to] control transactions that occur wholly outside of the State after ... medical waste ... has been removed from the State"); *Sam Francis Found. v. Christies, Inc.*, 784 F.3d 1320, 1323 (9th Cir. 2015) ("easily conclud[ing] that" dormant Commerce Clause was violated by use of California statute to regulate terms of art sales outside the state simply because seller resided in California).

Christies is instructive. That case involved California's Resale Royalty Act, which required a seller of fine art to pay the artist a 5% royalty "if the seller resides in California or the sale takes place in California." *Id.* (citation omitted). Various artists sued auction houses and an online retailer for violating the Royalty Act by failing to pay the required royalties on fine art sales, alleging "some sales took place in California and that other sales took place outside California but on behalf of a seller who is a resident of California." *Id.* at 1322. The Ninth Circuit affirmed the district court's Rule 12(b)(6) dismissal of the plaintiffs' claims:

Davis Wright Tremaine LLP
LAW OFFICES
920 Fifth Avenue, Suite 3300
Seattle, WA 98104-1610
206.622.3150 main · 206.757.7700 fax

> [The] Royalty Act requires the payment of royalties to the artist after a sale of fine art whenever "the seller resides in California *or* the sale takes place in California." Defendants challenge the first clause because it regulates sales that take place outside California. ***Those sales have no necessary connection with the state other than the residency of the seller***. For example, if a California resident has a part-time apartment in New York, buys a sculpture in New York from a North Dakota artist to furnish her apartment, and later sells the sculpture to a friend in New York, the Act requires the payment of a royalty to the North Dakota artist – even if the sculpture, the artist, and the buyer never traveled to, or had any connection with, California. ***We easily conclude that the royalty requirement, as applied to out-of-state sales by California residents, violates the dormant Commerce Clause***. . . .

Id. at 1323–24 (emphasis added) (internal citations omitted).

Plaintiffs' BIPA claims present analogous circumstances: like the California-based art sellers in *Christies*, Plaintiffs' Illinois residency does not allow them to use BIPA to regulate the transmission of data between two non-Illinois entities (*i.e.*, IBM and Microsoft) simply because some of the data purportedly relates to Illinois residents.

Courts that have found dormant Commerce Clause challenges premature at the pleading stage in BIPA cases have done so based on very different allegations. In finding Shutterfly's dormant Commerce Clause argument premature at the pleading stage, for example, the *Monroy* court emphasized plaintiff's "suit, as well as his proposed class, is confined to individuals whose biometric data was obtained from photographs ***uploaded to Shutterfly in Illinois***." 2017 WL 4099846, at *7 (emphasis added). As a result, "[a]pplying BIPA in this case would not entail any regulation of Shutterfly's gathering and storage of biometric data obtained outside of Illinois." *Id.* By contrast, based on the allegations in the Complaint here, "applying BIPA in this case ***would*** [] entail [] regulation of [Microsoft's alleged] gathering and storage of biometric data obtained outside of Illinois" because Plaintiffs do not allege they uploaded their photographs to Microsoft, much less to Microsoft (or IBM) in Illinois. *See id.* (emphasis added).

Davis Wright Tremaine LLP
LAW OFFICES
920 Fifth Avenue, Suite 3300
Seattle, WA 98104-1610
206.622.3150 main · 206.757.7700 fax

2. Plaintiffs' BIPA Claims Impermissibly Displace the Legislation and Policy Decisions Made by States Other Than Illinois.

The dormant Commerce Clause also prevents "inconsistent legislation arising from the projection of one state regulatory regime into the jurisdiction of another State." *Healy*, 491 U.S. at 337. This has particular application where, as here, extraterritorial application of Illinois law would ***displace*** the inconsistent policies of other states, including Washington, where Microsoft is incorporated and has its principal place of business.

Washington has its own Biometric Privacy Law, which applies only to the use and collection of biometric information for "commercial purposes." RCW 19.375.020(1). Plaintiffs do not allege Microsoft violated the Washington law. They do not allege Microsoft used their biometrics for a "[c]ommercial purpose" as narrowly defined in Washington: "a purpose in furtherance of the sale or disclosure to a third party of a biometric identifier for the purpose of marketing of goods or services when such goods or services are unrelated to the initial transaction in which a person first gains possession of an individual's biometric identifier." RCW 19.375.010(4). Further, Washington's law defines "[b]iometric identifier" as "data generated by automatic measurements of an individual's biological characteristics . . . used to identify a specific individual," but specifically excludes "a ***physical or digital photograph . . . or data generated therefrom***" from the definition. RCW 19.375.010(1) (emphasis added). In other words, Washington's law specifically ***excludes*** from its scope the facial-recognition technology alleged in the Complaint. *See* Compl. ¶¶ 41–44 (alleging "biometric identifiers and information" in IBM's DiF Dataset were obtained from photos).

Washington's and Illinois's statutes not only differ in reach, but also establish inconsistent requirements. Illinois imposes notice and consent requirements on any businesses that "collect, capture, purchase, receive through trade, or otherwise obtain a person's ... biometric identifier or biometric information," without regard to the purpose of the collection. 740 ILCS 14/15(b). In contrast, Washington requires notice and consent only to

Davis Wright Tremaine LLP
LAW OFFICES
920 Fifth Avenue, Suite 3300
Seattle, WA 98104-1610
206.622.3150 main · 206.757.7700 fax

"enroll" biometric information in a database—which "enrollment" activity Plaintiffs do not allege Microsoft has engaged in—involving "captur[ing] a biometric identifier of an individual, convert[ing] it into a reference template that cannot be reconstructed into the original output image, and stor[ing] it in a database that matches the biometric identifier to a specific individual." RCW 19.375.020; RCW 19.375.010(5). Moreover, Washington law regulates the storage of biometric data only for a narrowly defined type of "commercial purpose," i.e., "in furtherance of the sale or disclosure to a third party of a biometric identifier for the purpose of marketing of goods or services." RCW 19.375.010(4). As a result, the Washington law does not reach Microsoft's conduct as alleged in the Complaint. Further, were the Court to interpret BIPA as applying to information obtained from photos (which it should not, for reasons explained below), the Illinois law would again conflict with Washington law, given Washington's explicit decision not to regulate a private entity's use of "data generated" from "a physical or digital photograph." RCW 19.375.010(1).

Allowing Plaintiffs' BIPA claims to proceed despite these differences between the Washington Biometric Privacy Law and BIPA would effectively allow Illinois to make policy and legislative decisions for Washington, when Washington struck a different balance regarding biometric privacy. While Plaintiffs may argue the laws do not "conflict" because a company could simultaneously comply with both statutes, it could only do so by complying with the stricter statute (BIPA)—a result that would effectively "forc[e] [Washington] to alter [its] regulations to conform with the conflicting legislation"—i.e., BIPA. *Nat'l Solid Wastes Mgmt. Ass'n v. Meyer*, 63 F.3d 652, 660 n.9 (7th Cir. 1995).

The dormant Commerce Clause is not violated only where it is logically impossible to comply with the laws of different states. In *National Collegiate Athletic Association v. Miller*, 10 F.3d 633 (9th Cir. 1993), for example, Nevada's statute "require[d] any national collegiate athletic association to provide a Nevada institution, employee, student-athlete, or booster who is accused of a rules infraction" with "procedural due process protections," many of which

Davis Wright Tremaine LLP
LAW OFFICES
920 Fifth Avenue, Suite 3300
Seattle, WA 98104-1610
206.622.3150 main · 206.757.7700 fax

were "not included in the NCAA enforcement program." *Id*. at 637. The Nevada statute did not literally "conflict" with NCAA rules or the laws of other states; it was simply stricter in that it required additional protections. The Ninth Circuit nonetheless held the statute violated the dormant Commerce Clause, and explained what is meant by states having "inconsistent obligations":

> [S]uppose that state X required proof of an infraction beyond a reasonable doubt, while state Y only required clear and convincing evidence, and state Z required infractions to be proven by a preponderance of the evidence. Given that the NCAA must have uniform enforcement procedures in order to accomplish its fundamental goals, its operation would be disrupted because it could not possibly comply with all three statutes. ***Nor would it do to say that it need only comply with the most stringent burden of persuasion (beyond a reasonable doubt), for a state with a less stringent standard might well consider its standard a maximum as well as a minimum***. The serious risk of inconsistent obligations wrought by the extraterritorial effect of the Statute demonstrates why it constitutes a per se violation of the Commerce Clause.

Id. at 639–40 (emphasis added).

Applied here, BIPA and the Washington Biometric Privacy Law are similarly inconsistent because the "state with a less stringent" biometric privacy law—i.e., Washington—"might well consider its standard a maximum as well as a minimum." For instance, perhaps not wanting to hamper research and development in a state known for technological innovation, the Washington legislature may have consciously narrowed the scope of its law so companies do not cease technological development over fears of liability.

The dormant Commerce Clause protects businesses engaged in interstate commerce from precisely this kind of inconsistency between state statutes, which can "easily subject the [defendant] to conflicting requirements." *See, e.g.*, *id.* at 639. This principle is particularly important in the context of transactions over the Internet, such as Microsoft's alleged download of the IBM DiF Dataset. "[C]ourts have long recognized that certain types of commerce demand consistent treatment," and "[t]he Internet represents one of those areas": "[r]egulation by any single state can only result in chaos, because at least some states will

Davis Wright Tremaine LLP
LAW OFFICES
920 Fifth Avenue, Suite 3300
Seattle, WA 98104-1610
206.622.3150 main · 206.757.7700 fax

likely enact laws subjecting Internet users to conflicting obligations." *Am. Libraries Ass'n v. Pataki*, 969 F. Supp. 160, 181 (S.D.N.Y. 1997); *see also ACLU v. Johnson*, 194 F.3d 1149, 1162 (10th Cir. 1999). At the very least, the "massive liability brought on by conflicting applicable law could chill ... the rapidly expanding field of Internet commerce." *Archdiocese of St. Louis v. Internet Entm't Grp., Inc.*, 1999 WL 66022, at *3 (E.D. Mo. Feb. 12, 1999).

Applying Illinois's BIPA law to regulate an online transaction through which Microsoft, a Washington company, allegedly downloaded data from IBM, a New York-based company, would burden interstate commerce and violate the dormant Commerce Clause. *See Backpage.com, LLC v. McKenna*, 881 F. Supp. 2d 1262, 1285–86 (W.D. Wash. 2012) (Washington statute likely violated dormant Commerce Clause because, among other things, it would regulate "advertisement[s] … occurring entirely outside of the state," and the statute's proposed "screening process would constitute a significant and costly change to … corporations that have little to no connection with the State of Washington" and a "burden [that] would be exponentially exacerbated if every state were permitted to legislate its own requirements"). Microsoft's alleged download of the DiF Dataset, which IBM created "for the purpose of improving the ability of facial recognition systems to fairly and accurately identify all individuals," Compl. ¶ 40, would pass muster under Washington law. To apply BIPA to govern transactions of this nature would adversely affect businesses and universities across the country, who could be forced to stop research into facial recognition using any dataset that might contain a small percentage of images of Illinois residents. *See, e.g.*, Ira Kemelmacher-Shlizerman et al., *The MegaFace Benchmark: 1 Million Faces for Recognition at Scale*, UNIVERSITY OF WASHINGTON (2015), http://megaface.cs.washington.edu/KemelmacherMegaFaceCVPR16.pdf, at § 3 (explaining University of Washington's "MegaFace" facial-recognition research project made use of "Yahoo's 100M Flickr set"). The dormant Commerce Clause exists precisely to prevent this burden on interstate commerce.

Davis Wright Tremaine LLP
LAW OFFICES
920 Fifth Avenue, Suite 3300
Seattle, WA 98104-1610
206.622.3150 main · 206.757.7700 fax

C. Plaintiffs Fail to State a Claim Under BIPA Sections 15(b) or 15(c).

Even if BIPA could apply to Microsoft's alleged conduct (and it does not), the claims would still fail because Plaintiffs state no claim under Sections 15(b) or (c), as BIPA does not reach photographs. Further, Plaintiffs improperly rely on mere passive possession of biometric identifiers or information, and do not plausibly plead Microsoft "profited" from their biometric identifiers or information.

1. BIPA Does Not Apply to the Use of Photographs.

Plaintiffs fail to state a claim under either BIPA Section 15(b) or 15(c) because, under the statute's plain language, it does not apply to photographs or identifiers derived from photographs. In enacting BIPA, the Illinois legislature created two categories of covered biometric data: (1) original sources of information about a person ("biometric identifiers"—defined as a "retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry"); and (2) data extracted or derived from those sources ("biometric information"—defined as "information . . . based on an individual's biometric identifier"). 740 ILCS 14/10. The statute specifically ***excludes*** photographs from the definition of "biometric identifier." And because "biometric information" includes ***only*** information based on a "biometric identifier," "information derived from" photographs necessarily cannot be "biometric information." *Id.*

In short, the Illinois legislature went out of its way to exclude both photographs and information derived from photographs from BIPA's scope. The alleged "comprehensive set of annotations of intrinsic facial features" IBM allegedly obtained from Plaintiffs' Flickr photos and made available to Microsoft (Compl. ¶¶ 41, 55) are therefore expressly excluded from the statutory definitions of "biometric identifier" and "biometric information."

The legislative history confirms BIPA's limited purpose. As BIPA moved toward passage, legislators narrowed the definitions of "biometric identifier" and "biometric information." The first Senate version defined "biometric identifier" broadly: "Examples of biometric identifiers ***include, but are not limited to***[,] iris or retinal scans, fingerprints,

Davis Wright Tremaine LLP
LAW OFFICES
920 Fifth Avenue, Suite 3300
Seattle, WA 98104-1610
206.622.3150 main · 206.757.7700 fax

voiceprints, and ***records*** of hand or facial geometry." Sen. Bill 2400, § 10 (Feb. 14, 2008) (emphasis added) (attached as **Exhibit A**).[4] And although the definition of "biometric identifier" always excluded "photographs," the original definition of "biometric information" did not exclude information ***derived from*** photographs. *Id.* The next proposal was even broader: "biometric identifier" included "records or scans of hand geometry, facial geometry, or ***facial recognition***." Sen. Am. to Sen. Bill 2400, § 10 (Apr. 11, 2008) (emphasis added) (attached as **Exhibit B**).

But that proposal was rejected, and the House offered a substantially narrower version: it (a) changed the definition of "biometric identifiers" from an open-ended set of "[e]xamples" to a narrow list of enumerated sources; (b) removed the broad term "records" of hand or face geometry; and (c) excluded from the definition of "biometric information" all "information derived from items or procedures excluded under the definition of biometric identifiers." House Am. to Sen. Bill 2400, § 10 (May 28, 2008) (attached as **Exhibit C**). The legislature enacted this narrower version of BIPA and expressly declined (a) to include a "record" of facial geometry in the definition of biometric identifier, (b) to regulate all forms of "facial recognition," or (c) to allow information derived from photographs to slip into the definition of "biometric information." This reflects a clear intent to regulate only a narrow set of technologies—and to exclude a host of others, including all forms of facial recognition derived from photographs.

Although some courts have declined to dismiss BIPA complaints where plaintiffs relied on the application of facial-recognition technology to photos, Microsoft respectfully submits those cases were wrongly decided, and this Court should decline to follow them. For

---

[4] The Court may take judicial notice of the legislative history attached as **Exhibits A–C**. *See, e.g.*, *Sonoma Cty. Ass'n of Retired Employees v. Sonoma Cty.*, 708 F.3d 1109, 1120 n.8 (9th Cir. 2013) (granting motion to take judicial notice of legislative history); *Harbers v. Eddie Bauer, LLC*, 415 F. Supp. 3d 999, 1007 n.5 (W.D. Wash. 2019) ("Information published on government websites, including legislative history, is a proper subject of judicial notice.").

Davis Wright Tremaine LLP
LAW OFFICES
920 Fifth Avenue, Suite 3300
Seattle, WA 98104-1610
206.622.3150 main · 206.757.7700 fax

example, the court in *In re Facebook Biometric Information Privacy Litigation*, 185 F. Supp. 3d 1155, 1171 (N.D. Cal. 2016), concluded "'[p]hotographs' is better understood to mean paper prints of photographs, not digitized images stored as a computer file and uploaded to the Internet." But this reading cannot be reconciled with the commonly understood meaning of "photograph" when the statute was passed in 2008. By 2006, even the Oxford English Dictionary defined "photograph" as "[a] picture made using a camera in which an image is focused on to sensitive material and then made visible and permanent by chemical treatment; (later also) ***a picture made by focusing an image and then storing it digitally***." Oxford English Dictionary (Mar. 2006), *available at* https://www.oed.com/view/Entry/142818?rskey=8jt7S7&result=1&isAdvanced=false#eid (emphasis added); *see also* Webster's Dictionary 373 (2008 ed.) ("photography" means "the art or process of producing images on a sensitive surface (as film or a CCD chip [a form of technology used in digital imaging] by the action of light") (attached as **Exhibit D)**.

A statutory term should be interpreted "consistent with standard definitions ... found in dictionaries, which [courts] may consult when attempting to ascertain the plain and ordinary meaning." *Rosenbach v. Six Flags Entm't Corp.*, 129 N.E.3d 1197, 1205 (Ill. 2019). By interpreting "[p]hotographs" to mean only "paper prints of photographs, not digitized images," 185 F. Supp. 3d at 1171, the court in *Facebook* ignored the "plain and ordinary meaning" of "photographs." The courts' reasoning in *Monroy* and *Rivera* is similarly unsound. Those cases did not properly account for BIPA Section 5, which makes clear the statute is intended to regulate "biometric identifier-facilitated ***transactions***," such as those that occur "at grocery stores, gas stations, and school cafeterias"—all intrinsically ***in-person*** activities. 740 ILCS 14/5(b)–(e) (emphasis added). Indeed, the statute gives several examples of the activities it regulates, and ***all*** involve in-person activities in which biometric information may be captured. *See id.*

The Court should also reject the reasoning of *Facebook*, *Monroy*, and *Rivera* because

Davis Wright Tremaine LLP
LAW OFFICES
920 Fifth Avenue, Suite 3300
Seattle, WA 98104-1610
206.622.3150 main · 206.757.7700 fax

that reasoning leads to absurd results. "[I]nterpretations of a statute which would produce absurd results are to be avoided if alternative interpretations consistent with the legislative purpose are available." *Griffin v. Oceanic Contractors, Inc.,* 458 U.S. 564, 575 (1982); *see also People v. Hanna,* 800 N.E.2d 1201, 1207–09 (Ill. 2003) (rejecting statutory construction leading to "absurd result" that regulated entity would be unable to comply with the statute's requirements). For example, the Complaint cites an article noting researchers have used facial-recognition technology "to identify the portraits of unknown soldiers in Civil War photographs taken in the 1860s." Compl. ¶ 54 n.15 (quoting Brad Smith, *Facial recognition: It's time for action* (Dec. 6, 2018), Microsoft, https://blogs.microsoft.com/on-the-issues/2018/12/06/facial-recognition-its-time-for-action/). Under the reasoning of *Facebook*, *Monroy*, and *Rivera*, using facial-recognition technology to scan soldiers' facial features for identification purposes leads to the creation of "biometric information," meaning a private entity cannot create this data without the subject's "written release." 740 ILCS 14/15(b). But a private entity obviously cannot obtain a "written release" from a Civil War veteran in an 1863 photo, and it begs credulity to assume the Illinois legislature meant for BIPA to prohibit such activity. This illustration, in addition to BIPA's "written release" requirement, shows BIPA contemplates in-person transactions involving use of biometric technology, not the creation of biometric data from a static image of an unidentified person.

2. Section 15(b) Does Not Apply to the Passive Possession of Data by Third Parties Like Microsoft.

BIPA Section 15(b) imposes the following requirements on private entities before they can collect an individual's biometric information: (1) inform the individual "in writing that a biometric identifier or biometric information is being collected"; (2) inform the individual "in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected"; and (3) receive "a written release executed by the subject." 740 ILCS 14/15(b). Unlike BIPA Sections 15(a), (c), (d), and (e)—which are triggered

Davis Wright Tremaine LLP
LAW OFFICES
920 Fifth Avenue, Suite 3300
Seattle, WA 98104-1610
206.622.3150 main · 206.757.7700 fax

through passive "possession"—only ***actions*** trigger Section 15(b), i.e., the private entity must "collect, capture, purchase, receive through trade," or "obtain" biometric information. 740 ILCS 14/15. Section 15(b) therefore does not impose any requirements on entities that merely "possess[]" biometric information, but only on entities who actively "collect" biometric information. Had the legislature meant to bring all entities who merely "possess" biometrics within Section 15(b)'s purview, it could have explicitly done so—as it did in Sections 15(a), (c), (d), and (e). *See, e.g.*, *Dana Tank Container, Inc. v. Human Rights Comm'n*, 687 N.E.2d 102, 104 (Ill. App. Ct. 1997) ("Where the legislature uses certain words in one instance and different words in another, it intended different results."); *accord In re D.W.*, 827 N.E.2d 466, 479 (Ill. 2005).

This textual difference confirms Section 15(b) does not apply to the conduct alleged here. Plaintiffs do not allege Microsoft collected or obtained biometric information directly from any individual, much less these Plaintiffs. *See, e.g.*, *Cameron v. Polar Tech Indus., Inc. & ADP, LLC*, No. 2019-CH-000013, Tr. at 29–36 (DeKalb Cty. Ill. Cir. Ct. Aug. 23, 2019) (dismissing Section 15(b) claim against third-party timekeeping vendor) (attached as **Exhibit E**); *Bernal v. ADP, LLC*, No. 2017-CH-12364, Order at 2–3 (Cook Cty. Ill. Cir. Ct. Aug. 23, 2019) (dismissing Section 15(a), (b), (c), and (d) claims against ADP and noting Section 15(b)'s "requirement that the private entity whose actions the subsection is meant to regulate must receive a 'written release' … does suggest that the legislature did not intend for the subsection to apply to a third party entity") (attached as **Exhibit F**); *Namuwonge v. Kronos, Inc.*, 418 F. Supp. 3d 279, 286 (N.D. Ill. 2019) (dismissing Section 15(b) claims against third-party timekeeping vendor and noting "there is a difference between *possessing* and *collecting* biometric information").

It would yield absurd results to construe Section 15(b) as imposing individual notice and release obligations on third parties like Microsoft, who do not collect ***any*** individual's biometric information but simply download a large dataset of anonymized images that, only

Davis Wright Tremaine LLP
LAW OFFICES
920 Fifth Avenue, Suite 3300
Seattle, WA 98104-1610
206.622.3150 main · 206.757.7700 fax

incidentally, ***may*** include some images of Illinois residents. Plaintiffs' proposed solution to this absurdity only compounds the problem. They allege Microsoft should have identified Plaintiffs' images by clicking the one million "links Defendant Microsoft received from IBM," ascertained each Plaintiff's photographs in the IBM DiF Dataset "originated from, and was affiliated with, his Flickr account," learned of Plaintiffs' Illinois residency by scrutinizing their accounts, and then contacted each Plaintiff to seek an individual release. Compl. ¶¶ 62-66 (Vance), 70-74 (Janecyk). Leaving aside the impracticality of this suggestion, it would not even satisfy Section 15(b) as Plaintiffs read it, because the statute forbids an entity's receipt of biometric information unless it "first" provides notice and secures a release. This, of course, is something the Complaint concedes Microsoft could not have done until ***after*** it had the IBM DiF dataset in its possession for a sufficient length of time to scour one million Flickr accounts, locate Plaintiffs, identify them as Illinois residents, and secure a release.

In short, under Plaintiffs' reading of the statute, no entity could safely download ***any*** large biometric dataset, no matter how anonymized the images or laudable the entity's purposes, because the specter of BIPA liability would loom large if the dataset happened to contain any images of Illinois residents—something the entity could ascertain only after it was too late to avoid liability. "[T]o read BIPA as requiring that a third party ..., without any direct relationship with [plaintiffs], obtain written releases from said [plaintiffs] would be unquestionably not only inconvenient but arguably absurd." *Bernal*, No. 2017-CH-12364, Ex. G at 2–3. The Court should dismiss Plaintiffs' BIPA Section 15(b) claim because they do not allege Microsoft actively collected or obtained their biometrics.

3. Plaintiffs Fail to Plausibly Allege Microsoft "Profited" From Their Biometrics and Thus Fail to Plead a Section 15(c) Claim.

Plaintiffs' BIPA Section 15(c) claim—based on Microsoft allegedly "profiting" from their biometrics by supposedly using the IBM DiF Database to improve its facial-recognition technology, *see* Compl. ¶ 58—turns on a mischaracterization of "profit" under Section 15(c).

Davis Wright Tremaine LLP
LAW OFFICES
920 Fifth Avenue, Suite 3300
Seattle, WA 98104-1610
206.622.3150 main · 206.757.7700 fax

That section provides an entity may not "sell, lease, trade, or otherwise profit from a person's ... biometric identifier or biometric information." The four verbs—"sell, lease, trade, or otherwise profit"—all contemplate the direct provision of biometric data in exchange for money. 740 ILCS 14/15(c). "[W]hen a statutory clause specifically describes several classes of ... things and then includes 'other ... things,' the word 'other' is interpreted to mean 'other such like.'" *Pooh-Bah Enter., Inc. v. Cnty. of Cook,* 905 N.E.2d 781, 799 (Ill. 2009). Thus, like "sell," "lease," and "trade," Section 15(c)'s use of "otherwise profit" contemplates an entity receiving a pecuniary benefit in exchange for a person's biometric data—not the indirect "profit" gained by using a large dataset of information derived from anonymous facial imagery "to improve the fairness and accuracy of ... facial recognition." Compl. ¶ 57.

Nothing in the Complaint plausibly suggests Microsoft profited from Plaintiffs' biometric data. For that reason, the Court should dismiss Plaintiffs' Section 15(c) claim.

II. THE COURT SHOULD DISMISS THE UNJUST ENRICHMENT CLAIM.

Plaintiffs must plead three elements to allege unjust enrichment under Washington law: "(1) that Microsoft received a benefit, (2) at [Plaintiffs'] expense, and (3) the circumstances make it unjust for Microsoft to retain the benefit without payment." *Cousineau v. Microsoft Corp*., 992 F. Supp. 2d 1116, 1129 (W.D. Wash. 2012) (Coughenour, J.) (citing *Young v. Young*, 164 Wn.2d 477 (2008)). Illinois law is no different. S*ee Cleary v. Philip Morris Inc*., 656 F.3d 511, 516 (7th Cir. 2011) (quoting *HPI Health Care Servs., Inc. v. Mt. Vernon Hosp., Inc*., 545 N.E.2d 672, 679 (Ill. 1989)) ("In Illinois, '[t]o state a cause of action based on a theory of unjust enrichment, a plaintiff must allege that the defendant has unjustly retained a benefit to the plaintiff's detriment, and that defendant's retention of the benefit violates the fundamental principles of justice, equity, and good conscience.'"). "In the absence of a conflict [between Illinois and Washington law], Washington law applies" because it is the law of the forum state. *Kelley v. Microsoft Corp.*, 251 F.R.D. 544, 550 (W.D. Wash. 2008).

Davis Wright Tremaine LLP
LAW OFFICES
920 Fifth Avenue, Suite 3300
Seattle, WA 98104-1610
206.622.3150 main · 206.757.7700 fax

The Court should dismiss Plaintiffs' unjust enrichment claim for at least three reasons.

First, as explained above, the conduct at issue does not violate any applicable law, and Plaintiffs have not alleged anything independent of BIPA that would make Microsoft's alleged conduct "inequitable." In fact, nothing in the Complaint suggests Plaintiffs' Flickr photos were privately posted; to the contrary, Plaintiffs suggest their images were publicly available to anyone. *See* Compl. ¶¶ 64, 72.

Second, although Plaintiffs allege the IBM DiF Dataset, consisting of a million images, indirectly "enriched" Microsoft by playing some undefined role in "improv[ing] its facial recognition products," Compl. ¶ 58, they do not allege this purported enrichment caused them to suffer a corresponding economic "expense" or "detriment." This Court has rejected the notion that unjust enrichment can be based on alleged misuse of personal or private data because unjust enrichment does not apply "outside the context of an 'expense' stemming from some tangible economic loss to a plaintiff." *Cousineau*, 992 F. Supp. 2d at 1129-30 (granting motion to dismiss unjust enrichment claim that Microsoft used location data "to improve its systems and develop its mobile marketing campaign"); *see also Mount v. PulsePoint, Inc.*, 684 Fed. App'x 32, 36 (2d Cir. 2017), *as amended* (May 3, 2017) (plaintiffs failed to plead unjust enrichment in light of "plaintiffs' failure to allege specific loss or deprivation of opportunity to profit from [personal] information"); *Welborn v. Internal Revenue Serv.*, 218 F. Supp. 3d 64, 78 (D.D.C. 2016) (collecting cases for observation "[c]ourts have routinely rejected the proposition that an individual's personal identifying information has an independent monetary value").

Third, unjust enrichment provides an equitable remedy, available only when a plaintiff lacks an adequate remedy at law. As a result, when plaintiffs have a statutory remedy available, "they are not entitled to pursue a remedy in equity" for unjust enrichment. *Seattle Prof'l Eng'g Employees Ass'n v. Boeing Co.*, 139 Wn.2d 824, 838–39 (2000) (employees who "had a cause of action under chapter 49.52 RCW" could not pursue equitable claim for

Davis Wright Tremaine LLP
LAW OFFICES
920 Fifth Avenue, Suite 3300
Seattle, WA 98104-1610
206.622.3150 main · 206.757.7700 fax

restitution or unjust enrichment). Here, no common law principle makes it unfair or inequitable for an entity "to improve the fairness and accuracy of its facial recognition products and technologies," Compl. ¶ 57, by using biometric markers derived from a large dataset of photographs. Plaintiffs' unjust enrichment claim therefore turns on their allegation of a BIPA violation. In the circumstances, Plaintiffs must pursue their remedies at law, under BIPA, or not at all.

III. PLAINTIFFS HAVE NO SEPARATE INJUNCTIVE RELIEF CLAIM.

Plaintiffs' purported cause of action for injunctive relief fails because "[i]njunctive relief is a remedy, not a cause of action." *Edifecs Inc., v. TIBCO Software Inc.*, 2011 WL 1045645, at *3 (W.D. Wash. Mar. 23, 2011). The Court should also dismiss the request for injunctive relief because Plaintiffs fail to plead viable causes of action in Counts I through III and, therefore, have no valid claim to which they could tie the requested remedy of injunctive relief. *See, e.g.*, *Edwards v. JPMorgan Chase Bank, N.A.*, 2011 WL 3516155, at *3–4 (W.D. Wash. Aug. 11, 2011) (dismissing injunctive relief claim and noting plaintiffs "have no right to injunctive relief absence a viable cause of action against [defendant]").

CONCLUSION

For the foregoing reasons, Microsoft respectfully requests that the Court dismiss Plaintiffs' Complaint with prejudice.

DATED this 14th day of September, 2020.

DAVIS WRIGHT TREMAINE LLP
Attorneys for Defendant Microsoft Corporation

By */s/ Stephen M. Rummage*
Stephen M. Rummage, WSBA #11168
Xiang Li, WSBA #52306
920 Fifth Avenue, Suite 3300
Seattle, WA 98104-1610
Telephone: (206) 757-8136
Fax: (206) 757-7136
E-mail: steverummage@dwt.com
xiangli@dwt.com

MORGAN LEWIS & BOCKIUS
Attorneys for Defendant Microsoft Corporation

By */s/ Elizabeth B. Herrington*
Elizabeth B. Herrington (*pro hac vice*)
Tyler Zmick (*pro hac vice*)
77 West Wacker Drive, Suite 500
Chicago, IL 60601-5094
Telephone: (312) 324-1188
E-mail:
beth.herrington@morganlewis.com
tyler.zmick@morganlewis.com

Davis Wright Tremaine LLP
LAW OFFICES
920 Fifth Avenue, Suite 3300
Seattle, WA 98104-1610
206.622.3150 main · 206.757.7700 fax

Exhibit A

SB2400

LRB095 19768 KBJ 46142 b

95TH GENERAL ASSEMBLY

State of Illinois

2007 and 2008

SB2400

Introduced 2/14/2008, by Sen. Terry Link

SYNOPSIS AS INTRODUCED:

New Act

Creates the Biometric Information Privacy Act. Provides that a public agency or private entity in possession of biometric identifiers or biometric information must develop a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within 3 years of the individual's last interaction with the public agency or private entity. Provides that absent a valid warrant or subpoena, a public agency or private entity in possession of biometric identifiers or biometric information must comply with its established retention schedule and destruction guidelines. Provides that no public agency or private entity may collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifier or biometric information, unless it first satisfies certain conditions. Provides that these provisions do not apply to a public agency engaged in criminal investigations or prosecutions or a public agency acting pursuant to a valid warrant or subpoena. Provides that a public agency in possession of biometric identifiers or biometric information shall store, transmit, and protect from disclosure all biometric identifiers and biometric information in a manner that is the same as or more protective than the manner in which the public agency stores, transmits, and protects other confidential and sensitive information. Provides that any person aggrieved by a violation of this Act shall have a right of action in a State circuit court or as a supplemental claim in federal district court. Preempts home rule. Contains other provisions.

LRB095 19768 KBJ 46142 b

FISCAL NOTE ACT MAY APPLY

HOME RULE NOTE ACT MAY APPLY

A BILL FOR

AN ACT concerning health.

Be it enacted by the People of the State of Illinois, represented in the General Assembly:

Section 1. Short title. This Act may be cited as the Biometric Information Privacy Act.

Section 5. Legislative findings; intent. The General Assembly finds all of the following:

(a) The use of biometrics is growing in the business and security screening sectors and appears to promise streamlined financial transactions and security screenings.

(b) Major national corporations have selected the City of Chicago and other locations in this State as pilot testing sites for new applications of biometric-facilitated financial transactions, including "Pay By Touch" at banks, grocery stores, gas stations, and school cafeterias.

(c) Biometrics are unlike other unique identifiers that are used to access finances or other sensitive information. For example, social security numbers, when compromised, can be changed. Biometrics, however, are biologically unique to the individual; therefore, once compromised, the individual has no recourse, is at heightened risk for identity theft, and is likely to withdraw from biometric-facilitated transactions.

(d) An overwhelming majority of members of the public are

opposed to the use of biometrics when such information is tied to personal finances and other personal information.

(e) Despite limited State law regulating the collection, use, safeguarding, and storage of biometric information, many members of the public are deterred from partaking in biometric identifier-facilitated facility transactions.

(f) The public welfare, security, and safety will be served by regulating the collection, use, safeguarding, handling, storage, retention, and destruction of biometric identifiers and information.

Section 10. Definitions. In this Act:

"Biometric identifier" means any indelible personal physical characteristic which can be used to uniquely identify an individual or pinpoint an individual at a particular place at a particular time. Examples of biometric identifiers include, but are not limited to iris or retinal scans, fingerprints, voiceprints, and records of hand or facial geometry. Biometric identifiers do not include writing samples, written signature, and photographs.

"Biometric information" means any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual.

"Confidential and sensitive information" means personal information that can be used to uniquely identify an individual

or an individual's account or property include, but are not limited to a genetic marker, genetic testing information, a unique identifier number to locate an account or property, an account number, a PIN number, a pass code, a driver's license number, or a social security number.

"Legally effective written release" means informed written consent.

"Private entity" means any individual, partnership, corporation, limited liability company, association, or other group, however organized.

"Public agency" means the State of Illinois and its various subdivisions and agencies, and all units of local government, school districts, and other governmental entities.

Section 15. Retention; collection; disclosure; destruction.

(a) A public agency or private entity in possession of biometric identifiers or biometric information must develop a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within 3 years of the individual's last interaction with the public agency or private entity. Absent a valid warrant or subpoena issued by a court of competent jurisdiction, a public agency or private entity in

possession of biometric identifiers or biometric information must comply with its established retention schedule and destruction guidelines.

(b) No public agency or private entity may collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifier or biometric information, unless it first:

(1) informs the subject in writing that a biometric identifier or biometric information is being collected or stored;

(2) informs the subject in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used; and

(3) receives a legally effective written release executed by the subject of the biometric identifier or biometric information or the subject's legally authorized representative.

(c) Subsections (a) and (b) of this Section do not apply to a public agency engaged in criminal investigations or prosecutions. Subsections (a) and (b) of this Section do not apply to a public agency acting pursuant to a valid warrant or subpoena issued by a court of competent jurisdiction.

(d) No public agency or private entity in possession of a biometric identifier or biometric information may sell, lease, trade, or otherwise profit from a person's or a customer's

biometric identifier or biometric information.

(e) Nothing in subsection (d) of this Section shall be construed to prohibit or inhibit a public agency engaged in criminal investigations or prosecutions from:

(1) sharing biometric identifiers or biometric information with another public agency engaged in criminal investigations or prosecutions to further such criminal investigations or prosecutions;

(2) sharing biometric identifiers or biometric information pursuant to federal law or regulation; or

(3) sharing biometric identifiers or biometric information pursuant to a valid warrant or subpoena issued by a court of competent jurisdiction.

(f) No public agency, private entity, or person in possession of a biometric identifier or biometric information may disclose, redisclose, or otherwise disseminate a person's or a customer's biometric identifier or biometric information, unless:

(1) the subject of the biometric identifier or biometric information or the subject's legally authorized representative consents to the disclosure or redisclosure;

(2) the disclosure or redisclosure completes a financial transaction requested or authorized by the subject of the biometric identifier or the biometric information;

(3) the disclosure or redisclosure is required under

federal law; and

(4) the disclosure is required pursuant to a valid warrant or subpoena issued by a court of competent jurisdiction.

(g) A public agency in possession of biometric identifiers or biometric information shall store, transmit, and protect from disclosure all biometric identifiers and biometric information in a manner that is the same as or more protective than the manner in which the public agency stores, transmits, and protects other confidential and sensitive information.

(h) A private entity in possession of a biometric identifier or biometric information shall:

(1) store, transmit, and protect from disclosure all biometric identifiers and biometric information using the reasonable standard of care within the private entity's industry; and

(2) store, transmit, and protect from disclosure all biometric identifiers and biometric information in a manner that is the same as or more protective than the manner in which the private entity stores, transmits, and protects other confidential and sensitive information.

(i) All information and records held by a public agency pertaining to biometric identifiers and biometric information shall be confidential and exempt from copying and inspection under the Freedom of Information Act to all except to the subject of the biometric identifier or biometric information.

The subject of the biometric identifier or biometric information held by a public agency shall be permitted to copy and inspect only their own biometric identifiers and biometric information.

Section 20. Right of action.

(a) Any person aggrieved by a violation of this Act shall have a right of action in a State circuit court or as a supplemental claim in federal district court against an offending party. A prevailing party may recover for each violation:

(1) against any public agency or private entity that negligently violates a provision of this Act, liquidated damages of $1,000 or actual damages, whichever is greater;

(2) against any public agency or private entity that intentionally or recklessly violates a provision of this Act, liquidated damages of $5,000 or actual damages, whichever is greater;

(3) reasonable attorneys' fees and costs, including expert witness fees and other litigation expenses; and

(4) other relief, including an injunction, as the State or federal court may deem appropriate.

(b) For the purpose of this Act, "prevailing party" includes any party: (i) who obtains some of his or her requested relief through a judicial judgment in his or her favor; (ii) who obtains some of his or her requested relief

through any settlement agreement approved by the court; or (iii) whose pursuit of a non-frivolous claim was a catalyst for a unilateral change in position by the opposing party relative to the relief sought.

Section 25. Home rule. The corporate authorities of a municipality or other unit of local government may enact ordinances, standards, rules, or regulations that protect biometric identifiers and biometric information in a manner or to an extent equal to or greater than the protection provided in this Act. This Section is a limitation on the concurrent exercise of home rule power under subsection (i) of Section 6 of Article VII of the Illinois Constitution.

Exhibit B

Sen. Terry Link

Filed: 4/11/2008

AMENDMENT TO SENATE BILL 2400

AMENDMENT NO. _____. Amend Senate Bill 2400, AS AMENDED, by replacing everything after the enacting clause with the following:

"Section 1. Short title. This Act may be cited as the Biometric Information Privacy Act.

Section 5. Legislative findings; intent. The General Assembly finds all of the following:

(a) The use of biometrics is growing in the business and security screening sectors and appears to promise streamlined financial transactions and security screenings.

(b) Major national corporations have selected the City of Chicago and other locations in this State as pilot testing sites for new applications of biometric-facilitated financial transactions, including "Pay By Touch" at banks, grocery stores, gas stations, and school cafeterias.

(c) Biometrics are unlike other unique identifiers that are used to access finances or other sensitive information. For example, social security numbers, when compromised, can be changed. Biometrics, however, are biologically unique to the individual; therefore, once compromised, the individual has no recourse, is at heightened risk for identity theft, and is likely to withdraw from biometric-facilitated transactions.

(d) An overwhelming majority of members of the public are opposed to the use of biometrics when such information is tied to personal finances and other personal information.

(e) Despite limited State law regulating the collection, use, safeguarding, and storage of biometric information, many members of the public are deterred from partaking in biometric identifier-facilitated facility transactions.

(f) The public welfare, security, and safety will be served by regulating the collection, use, safeguarding, handling, storage, retention, and destruction of biometric identifiers and information.

Section 10. Definitions. In this Act:

"Biometric identifier" means any indelible personal physical characteristic which can be used to uniquely identify an individual or pinpoint an individual at a particular place at a particular time. Examples of biometric identifiers include, but are not limited to iris or retinal scans, fingerprints, voiceprints, and records or scans of hand

geometry, facial geometry, or facial recognition. Biometric identifiers do not include writing samples, written signatures, photographs, tattoo descriptions, physical descriptions, or human biological samples used for valid scientific testing or screening. Biometric identifiers do not include donated organs, tissues, or parts as defined in the Illinois Anatomical Gift Act or blood or serum stored on behalf of recipients or potential recipients of living or cadaveric transplants and obtained or stored by a federally-designated organ procurement agency. Biometric identifiers do not include biological materials regulated under the Genetic Information Privacy Act. Biometric identifiers do not include information captured from a patient in a health care setting or information collected, used, or stored for health care treatment, payment, or operations under the federal Health Insurance Portability and Accountability Act of 1996. Biometric identifiers do not include an X-ray, roentgen process, computed tomography, MRI, PET scan, mammography, or other image or film of the human anatomy used to diagnose, prognose, or treat an illness or other medical condition or to further valid scientific testing or screening.

"Biometric information" means any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual. Biometric information does not include information derived from items or procedures excluded under the definition

of biometric identifiers. Biometric information does not include information captured from a patient in a health care setting or information collected, used, or stored for health care treatment, payment, or operations under the federal Health Insurance Portability and Accountability Act of 1996.

"Confidential and sensitive information" means personal information that can be used to uniquely identify an individual or an individual's account or property. Examples of confidential and sensitive information include, but are not limited to, a genetic marker, genetic testing information, a unique identifier number to locate an account or property, an account number, a PIN number, a pass code, a driver's license number, or a social security number.

"Legally effective written release" means informed written consent or a release executed by an employee as a condition of employment.

"Private entity" means any individual, partnership, corporation, limited liability company, association, or other group, however organized. A private entity does not include a public agency. A private entity does not include any court of Illinois, a clerk of the court, or a judge or justice thereof.

"Public agency" means the State of Illinois and its various subdivisions and agencies, and all units of local government, school districts, and other governmental entities. A public agency does not include any court of Illinois, a clerk of the court, or a judge or justice thereof.

Section 15. Retention; collection; disclosure; destruction.

(a) A public agency or private entity in possession of biometric identifiers or biometric information must develop a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within 3 years of the individual's last interaction with the public agency or private entity, whichever occurs first. Absent a valid warrant or subpoena issued by a court of competent jurisdiction, a public agency or private entity in possession of biometric identifiers or biometric information must comply with its established retention schedule and destruction guidelines.

(b) No public agency or private entity may collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifier or biometric information, unless it first:

(1) informs the subject in writing that a biometric identifier or biometric information is being collected or stored;

(2) informs the subject in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and

used; and

(3) receives a legally effective written release executed by the subject of the biometric identifier or biometric information or the subject's legally authorized representative.

(c) Subsections (a) and (b) of this Section do not apply to a public agency:

(1) engaged in criminal investigations, arrests, prosecutions, or law enforcement;

(2) overseeing pretrial detention, post-trial commitment, corrections or incarceration, civil commitment, probation services, or parole services;

(3) serving as the State central repository of biometrics for criminal identification and investigation purposes;

(4) furnishing biometric identifiers or biometric information to a State or federal repository of biometrics pursuant to State or federal law or municipal ordinance;

(5) receiving biometric identifiers or biometric information pursuant to State or federal law or municipal ordinance;

(6) acting pursuant to a valid warrant or subpoena issued by a court of competent jurisdiction;

(7) issuing driver's licenses, driver's permits, identification cards issued pursuant to the Illinois Identification Card Act, or occupational licenses; or

(8) performing employee background checks in accordance with the public agency's hiring policies or statutory obligations.

Nothing in subsections (a) and (b) of this Section shall be construed to conflict with the retention and collection practices for fingerprints, other biometric identifiers, or biometric information under the Criminal Identification Act, the Illinois Uniform Conviction Information Act, or the federal National Crime Prevention and Privacy Compact. Subsection (a) of this Section does not apply to school districts; however, a school district that collects biometric identifiers or biometric information must adopt retention schedules and destruction policies in accordance with the School Code. Subsection (a) of this Section does not apply to a fingerprint vendor or fingerprint vendor agency; however, a fingerprint vendor or fingerprint vendor agency must adopt retention schedules and destruction polices in accordance with the Private Detective, Private Alarm, Private Security, Fingerprint Vendor, and Locksmith Act of 2004.

(d) No public agency or private entity in possession of a biometric identifier or biometric information may sell, lease, trade, or otherwise profit from a person's or a customer's biometric identifier or biometric information.

(e) No public agency or private entity in possession of a biometric identifier or biometric information may disclose, redisclose, or otherwise disseminate a person's or a customer's

biometric identifier or biometric information unless:

(1) the subject of the biometric identifier or biometric information or the subject's legally-authorized representative consents to the disclosure or redisclosure;

(2) the disclosure or redisclosure completes a financial transaction requested or authorized by the subject of the biometric identifier or the biometric information;

(3) the disclosure or redisclosure is required by State or federal law or municipal ordinance; or

(4) the disclosure is required pursuant to a valid warrant or subpoena issued by a court of competent jurisdiction.

(f) Nothing in subsections (d) or (e) of this Section shall be construed to prohibit or inhibit a public agency (i) engaged in criminal investigations, arrests, prosecutions, or law enforcement, (ii) overseeing pretrial detention, post-trial commitment, corrections or incarceration, civil commitment, probation services, or parole services, (iii) serving as the State central repository of biometrics for criminal identification and investigation purposes, (iv) furnishing biometric identifiers or biometric information to a State or federal repository of biometrics pursuant to State or federal law, or (v) issuing driver's licenses, driver's permits, or identification cards pursuant to the Illinois Identification Card Act from:

(1) sharing biometric identifiers or biometric information with another public agency engaged in criminal investigations, arrests, prosecutions, or law enforcement to further such criminal investigations, arrests, prosecutions, or law enforcement;

(2) sharing biometric identifiers or biometric or biometric information with another public agency overseeing pretrial detention, post-trial commitment, corrections or incarceration, civil commitment, probation services, or parole services;

(3) sharing biometric identifiers or biometric information pursuant to, or required by, State or federal law; or

(4) sharing biometric identifiers or biometric information pursuant to a valid warrant or subpoena issued by a court of competent jurisdiction.

(g) Nothing in subsections (d) or (e) of this Section shall be construed to conflict with the reporting and sharing practices for fingerprints, other biometric identifiers, or biometric information under the Criminal Identification Act, the Illinois Uniform Conviction Information Act, and the federal National Crime Prevention and Privacy Compact. Nothing in subsection (d) of this Section shall be construed to conflict with the reporting and sharing practices of a fingerprint vendor or fingerprint vendor agency under the Private Detective, Private Alarm, Private Security,

Fingerprint Vendor, and Locksmith Act of 2004.

(h) Nothing in subsections (d) or (e) of this Section shall be construed to prohibit or inhibit a public agency that issues occupational licenses from:

(1) sharing biometric identifiers or biometric information pursuant to or when required by State or federal law; or

(2) sharing biometric identifiers or biometric information pursuant to a valid warrant or subpoena issued by a court of competent jurisdiction.

(i) Nothing in subsections (d) or (e) of this Section shall be construed to prohibit a public agency from performing employee background checks in accordance with the public agency's hiring policies or statutory obligations.

(j) A public agency in possession of biometric identifiers or biometric information shall store, transmit, and protect from disclosure all biometric identifiers and biometric information in a reasonable manner that is the same as or more protective than the manner in which the public agency stores, transmits, and protects other similar confidential and sensitive information specific to that public agency. The storage, transmittal, and protection from disclosure standards under this subsection (j) are solely the choice of the public agency to adopt in accordance with this Act, other applicable State or federal law, evolving advances in technology, budget constraints, and comparable practices specific to that public

agency.

(k) A private entity in possession of a biometric identifier or biometric information shall:

(1) store, transmit, and protect from disclosure all biometric identifiers and biometric information using the reasonable standard of care within the private entity's industry; and

(2) store, transmit, and protect from disclosure all biometric identifiers and biometric information in a manner that is the same as or more protective than the manner in which the private entity stores, transmits, and protects other confidential and sensitive information.

(l) All information and records held by a public agency pertaining to biometric identifiers and biometric information shall be confidential and exempt from copying and inspection under the Freedom of Information Act to all except to the subject of the biometric identifier or biometric information. The subject of the biometric identifier or biometric information held by a public agency shall be permitted to copy and inspect only their own biometric identifiers and biometric information.

Section 20. Right of action. Any person aggrieved by a violation of this Act shall have a right of action in a State circuit court or as a supplemental claim in federal district court against an offending party. A prevailing party may

recover for each violation:

(1) against any public agency or private entity that negligently violates a provision of this Act, liquidated damages of $1,000 or actual damages, whichever is greater;

(2) against any public agency or private entity that intentionally or recklessly violates a provision of this Act, liquidated damages of $5,000 or actual damages, whichever is greater;

(3) reasonable attorneys' fees and costs, including expert witness fees and other litigation expenses; and

(4) other relief, including an injunction, as the State or federal court may deem appropriate.

Section 25. Construction. Nothing in this Act shall be construed to impact the admission or discovery of biometric identifiers and biometric information in any action of any kind in any court, or before any tribunal, board, agency, or person. Nothing in this Act shall be construed to conflict with the X-Ray Retention Act or the federal Health Insurance Portability and Accountability Act of 1996. Subcontractors or agents of a public agency must comply with this Act to the extent and manner this Act applies to that public agency.

Section 30. Home rule. Any home rule unit of local government, any non home rule municipality, or any non home rule county within the unincorporated territory of the county

may enact ordinances, standards, rules, or regulations that protect biometric identifiers and biometric information in a manner or to an extent equal to or greater than the protection provided in this Act. This Section is a limitation on the concurrent exercise of home rule power under subsection (i) of Section 6 of Article VII of the Illinois Constitution.

Section 95. Applicability. This Act applies to private entities beginning on the effective date of this Act. This Act applies to public agencies beginning on January 1, 2011.

Section 99. Effective date. This Act takes effect upon becoming law.".

Exhibit C

Executive Committee

Filed: 5/28/2008

AMENDMENT TO SENATE BILL 2400

AMENDMENT NO. _____. Amend Senate Bill 2400 by replacing everything after the enacting clause with the following:

"Section 1. Short title. This Act may be cited as the Biometric Information Privacy Act.

Section 5. Legislative findings; intent. The General Assembly finds all of the following:

(a) The use of biometrics is growing in the business and security screening sectors and appears to promise streamlined financial transactions and security screenings.

(b) Major national corporations have selected the City of Chicago and other locations in this State as pilot testing sites for new applications of biometric-facilitated financial transactions, including finger-scan technologies at grocery stores, gas stations, and school cafeterias.

(c) Biometrics are unlike other unique identifiers that are

used to access finances or other sensitive information. For example, social security numbers, when compromised, can be changed. Biometrics, however, are biologically unique to the individual; therefore, once compromised, the individual has no recourse, is at heightened risk for identity theft, and is likely to withdraw from biometric-facilitated transactions.

(d) An overwhelming majority of members of the public are weary of the use of biometrics when such information is tied to finances and other personal information.

(e) Despite limited State law regulating the collection, use, safeguarding, and storage of biometrics, many members of the public are deterred from partaking in biometric identifier-facilitated transactions.

(f) The full ramifications of biometric technology are not fully known.

(g) The public welfare, security, and safety will be served by regulating the collection, use, safeguarding, handling, storage, retention, and destruction of biometric identifiers and information.

Section 10. Definitions. In this Act:

"Biometric identifier" means a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry. Biometric identifiers do not include writing samples, written signatures, photographs, human biological samples used for valid scientific testing or screening, demographic data,

tattoo descriptions, or physical descriptions such as height, weight, hair color, or eye color. Biometric identifiers do not include donated organs, tissues, or parts as defined in the Illinois Anatomical Gift Act or blood or serum stored on behalf of recipients or potential recipients of living or cadaveric transplants and obtained or stored by a federally designated organ procurement agency. Biometric identifiers do not include biological materials regulated under the Genetic Information Privacy Act. Biometric identifiers do not include information captured from a patient in a health care setting or information collected, used, or stored for health care treatment, payment, or operations under the federal Health Insurance Portability and Accountability Act of 1996. Biometric identifiers do not include an X-ray, roentgen process, computed tomography, MRI, PET scan, mammography, or other image or film of the human anatomy used to diagnose, prognose, or treat an illness or other medical condition or to further validate scientific testing or screening.

"Biometric information" means any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual. Biometric information does not include information derived from items or procedures excluded under the definition of biometric identifiers.

"Confidential and sensitive information" means personal information that can be used to uniquely identify an individual

or an individual's account or property. Examples of confidential and sensitive information include, but are not limited to, a genetic marker, genetic testing information, a unique identifier number to locate an account or property, an account number, a PIN number, a pass code, a driver's license number, or a social security number.

"Private entity" means any individual, partnership, corporation, limited liability company, association, or other group, however organized. A private entity does not include a State or local government agency. A private entity does not include any court of Illinois, a clerk of the court, or a judge or justice thereof.

"Written release" means informed written consent or, in the context of employment, a release executed by an employee as a condition of employment.

Section 15. Retention; collection; disclosure; destruction.

(a) A private entity in possession of biometric identifiers or biometric information must develop a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within 3 years of the individual's last interaction with the private entity, whichever occurs first.

Absent a valid warrant or subpoena issued by a court of competent jurisdiction, a private entity in possession of biometric identifiers or biometric information must comply with its established retention schedule and destruction guidelines.

(b) No private entity may collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifier or biometric information, unless it first:

(1) informs the subject or the subject's legally authorized representative in writing that a biometric identifier or biometric information is being collected or stored;

(2) informs the subject or the subject's legally authorized representative in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used; and

(3) receives a written release executed by the subject of the biometric identifier or biometric information or the subject's legally authorized representative.

(c) No private entity in possession of a biometric identifier or biometric information may sell, lease, trade, or otherwise profit from a person's or a customer's biometric identifier or biometric information.

(d) No private entity in possession of a biometric

identifier or biometric information may disclose, redisclose, or otherwise disseminate a person's or a customer's biometric identifier or biometric information unless:

(1) the subject of the biometric identifier or biometric information or the subject's legally authorized representative consents to the disclosure or redisclosure;

(2) the disclosure or redisclosure completes a financial transaction requested or authorized by the subject of the biometric identifier or the biometric information or the subject's legally authorized representative;

(3) the disclosure or redisclosure is required by State or federal law or municipal ordinance; or

(4) the disclosure is required pursuant to a valid warrant or subpoena issued by a court of competent jurisdiction.

(e) A private entity in possession of a biometric identifier or biometric information shall:

(1) store, transmit, and protect from disclosure all biometric identifiers and biometric information using the reasonable standard of care within the private entity's industry; and

(2) store, transmit, and protect from disclosure all biometric identifiers and biometric information in a manner that is the same as or more protective than the manner in which the private entity stores, transmits, and

protects other confidential and sensitive information.

Section 20. Right of action. Any person aggrieved by a violation of this Act shall have a right of action in a State circuit court or as a supplemental claim in federal district court against an offending party. A prevailing party may recover for each violation:

(1) against a private entity that negligently violates a provision of this Act, liquidated damages of $1,000 or actual damages, whichever is greater;

(2) against a private entity that intentionally or recklessly violates a provision of this Act, liquidated damages of $5,000 or actual damages, whichever is greater;

(3) reasonable attorneys' fees and costs, including expert witness fees and other litigation expenses; and

(4) other relief, including an injunction, as the State or federal court may deem appropriate.

Section 25. Construction.

(a) Nothing in this Act shall be construed to impact the admission or discovery of biometric identifiers and biometric information in any action of any kind in any court, or before any tribunal, board, agency, or person.

(b) Nothing in this Act shall be construed to conflict with the X-Ray Retention Act, the federal Health Insurance Portability and Accountability Act of 1996 and the rules

promulgated under either Act.

(c) Nothing in this Act shall be deemed to apply in any manner to a financial institution or an affiliate of a financial institution that is subject to Title V of the federal Gramm-Leach-Bliley Act of 1999 and the rules promulgated thereunder.

(d) Nothing in this Act shall be construed to conflict with the Private Detective, Private Alarm, Private Security, Fingerprint Vendor, and Locksmith Act of 2004 and the rules promulgated thereunder.

Section 30. Home rule. Any home rule unit of local government, any non-home rule municipality, or any non-home rule county within the unincorporated territory of the county may enact ordinances, standards, rules, or regulations that protect biometric identifiers and biometric information in a manner or to an extent equal to or greater than the protection provided in this Act. This Section is a limitation on the concurrent exercise of home rule power under subsection (i) of Section 6 of Article VII of the Illinois Constitution.

Section 35. Biometric Information Privacy Study Committee.

(a) The Department of Human Services, in conjunction with Central Management Services, subject to appropriation or other funds made available for this purpose, shall create the Biometric Information Privacy Study Committee, hereafter

referred to as the Committee. The Department of Human Services, in conjunction with Central Management Services, shall provide staff and administrative support to the Committee. The Committee shall examine (i) current policies, procedures, and practices used by State and local governments to protect an individual against unauthorized disclosure of his or her biometric identifiers and biometric information when State or local government requires the individual to provide his or her biometric identifiers to an officer or agency of the State or local government; (ii) issues related to the collection, destruction, security, and ramifications of biometric identifiers, biometric information, and biometric technology; and (iii) technical and procedural changes necessary in order to implement and enforce reasonable, uniform biometric safeguards by State and local government agencies.

(b) The Committee shall hold such public hearings as it deems necessary and present a report of its findings and recommendations to the General Assembly before January 1, 2009. The Committee may begin to conduct business upon appointment of a majority of its members. All appointments shall be completed by 4 months prior to the release of the Committee's final report. The Committee shall meet at least twice and at other times at the call of the chair and may conduct meetings by telecommunication, where possible, in order to minimize travel expenses. The Committee shall consist of 27 members appointed as follows:

(1) 2 members appointed by the President of the Senate;

(2) 2 members appointed by the Minority Leader of the Senate;

(3) 2 members appointed by the Speaker of the House of Representatives;

(4) 2 members appointed by the Minority Leader of the House of Representatives;

(5) One member representing the Office of the Governor, appointed by the Governor;

(6) One member, who shall serve as the chairperson of the Committee, representing the Office of the Attorney General, appointed by the Attorney General;

(7) One member representing the Office of the Secretary of the State, appointed by the Secretary of State;

(8) One member from each of the following State agencies appointed by their respective heads: Department of Corrections, Department of Public Health, Department of Human Services, Central Management Services, Illinois Commerce Commission, Illinois State Police; Department of Revenue;

(9) One member appointed by the chairperson of the Committee, representing the interests of the City of Chicago;

(10) 2 members appointed by the chairperson of the Committee, representing the interests of other municipalities;

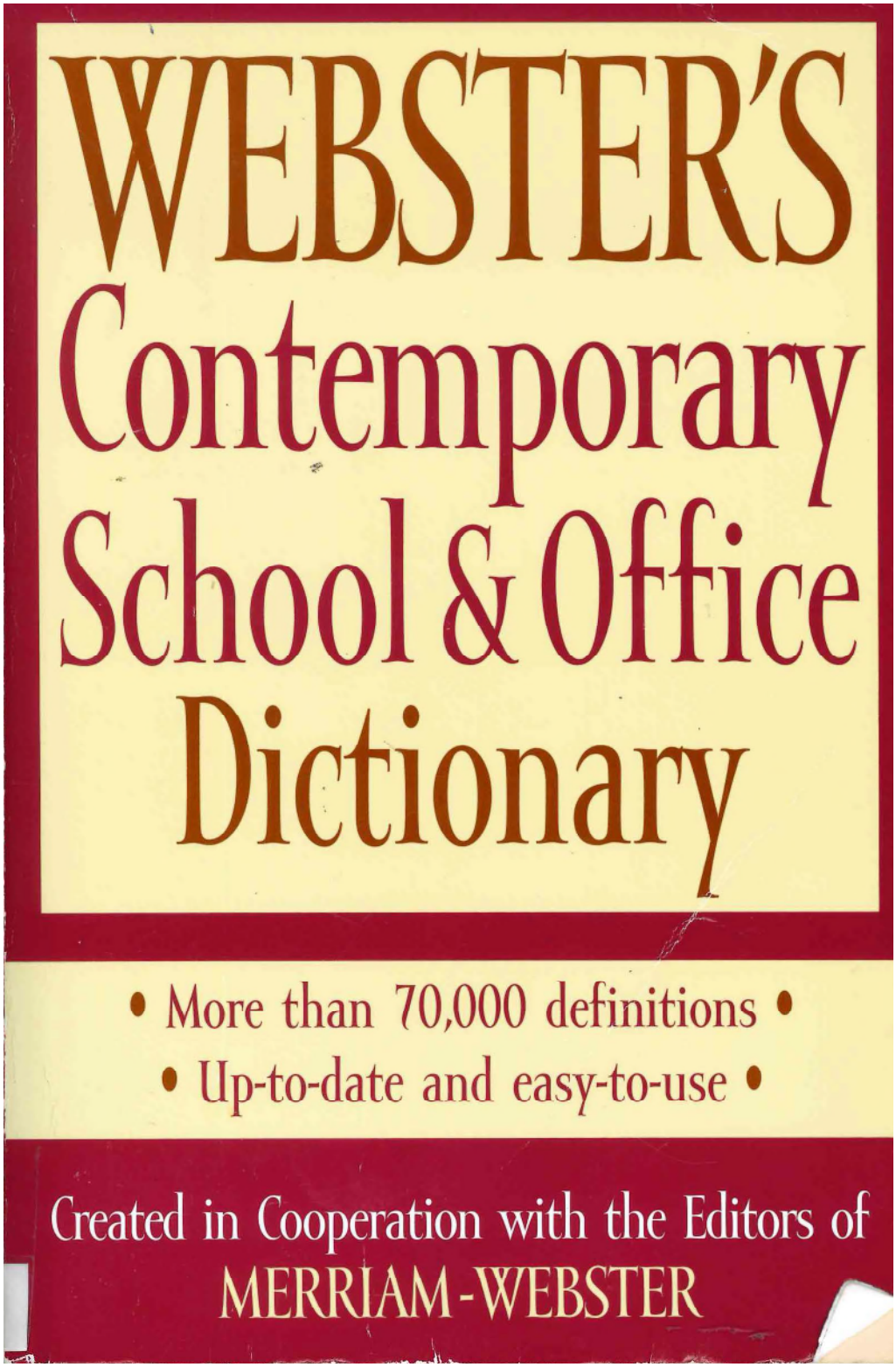
(11) 2 members appointed by the chairperson of the Committee, representing the interests of public hospitals; and

(12) 4 public members appointed by the chairperson of the Committee, representing the interests of the civil liberties community, the electronic privacy community, and government employees.

(c) This Section is repealed January 1, 2009.

Section 99. Effective date. This Act takes effect upon becoming law.".

Exhibit D


WEBSTER'S
Contemporary
School & Office
Dictionary
• More than 70,000 definitions •
• Up-to-date and easy-to-use •
Created in Cooperation with the Editors of
MERRIAM-WEBSTER

Webster's Contemporary School & Office Dictionary

Created in Cooperation with the Editors of
MERRIAM-WEBSTER

A Division of Merriam-Webster, Incorporated
Springfield, Massachusetts

This 2008 edition published by
Federal Street Press
A Division of Merriam-Webster, Incorporated
P.O. Box 281
Springfield, MA 01102

Federal Street Press books are available for bulk purchase for
sales promotion and premium use.
For details write the manager of special sales,
Federal Street Press, P.O. Box 281, Springfield, MA 01102

ISBN 13 978-1-59695-047-4

ISBN 10 1-59695-047-1

Printed in the United States of America

08 09 10 11 12 5 4 3 2 1

pho·to·chem·i·cal \ˌfō-tō-ˈke-mi-kəl\ *adj* : of, relating to, or resulting from the chemical action of radiant energy
pho·to·com·pose \-kəm-ˈpōz\ *vb* : to compose reading matter for reproduction by means of characters photographed on film — **pho·to·com·po·si·tion** \-ˌkäm-pə-ˈzi-shən\ *n*
pho·to·copy \ˈfō-tə-ˌkä-pē\ *n* : a photographic reproduction of graphic matter — **photocopy** *vb*
pho·to·elec·tric \ˌfō-tō-i-ˈlek-trik\ *adj* : relating to an electrical effect due to the interaction of light with matter — **pho·to·elec·tri·cal·ly** \-tri-k(ə-)lē\ *adv*
photoelectric cell *n* : a device whose electrical properties are modified by the action of light
pho·to·en·grave \ˌfō-tō-in-ˈgrāv\ *vb* : to make a photoengraving of
pho·to·en·grav·ing *n* : a process by which an etched printing plate is made from a photograph or drawing; *also* : a print made from such a plate
photo finish *n* : a race finish so close that a photograph of the finish is used to determine the winner
pho·tog \fə-ˈtäg\ *n* : PHOTOGRAPHER
pho·to·ge·nic \ˌfō-tə-ˈje-nik\ *adj* : eminently suitable esp. aesthetically for being photographed
pho·to·graph \ˈfō-tə-ˌgraf\ *n* : a picture taken by photography — **photograph** *vb* — **pho·tog·ra·pher** \fə-ˈtä-grə-fər\ *n*
pho·tog·ra·phy \fə-ˈtä-grə-fē\ *n* : the art or process of producing images on a sensitive surface (as film or a CCD chip by the action of light — **pho·to·graph·ic** \ˌfō-tə-ˈgra-fik\ *adj* — **pho·to·graph·i·cal·ly** \-fi-k(ə-)lē\ *adv*
pho·to·gra·vure \ˌfō-tə-grə-ˈvyůr\ *n* : a process for making prints from an intaglio plate prepared by photographic methods
pho·to·li·thog·ra·phy \ˌfō-tō-li-ˈthä-grə-fē\ *n* : the process of photographically transferring a pattern to a surface for etching (as in making an integrated circuit)
pho·tom·e·ter \fō-ˈtä-mə-tər\ *n* : an instrument for measuring the intensity of light — **pho·to·met·ric** \ˌfō-tə-ˈme-trik\ *adj* — **pho·tom·e·try** \fō-ˈtä-mə-trē\ *n*
pho·to·mi·cro·graph \ˌfō-tə-ˈmī-krə-ˌgraf\ *n* : a photograph of a microscope image — **pho·to·mi·crog·ra·phy** \-mī-ˈkrä-grə-fē\ *n*
pho·ton \ˈfō-ˌtän\ *n* : a quantum of electromagnetic radiation
photo op *n* : a situation or event that lends itself to the taking of pictures which favor the individuals photographed
pho·to·play \ˈfō-tō-ˌplā\ *n* : MOTION PICTURE
pho·to·sen·si·tive \ˌfō-tə-ˈsen-sə-tiv\ *adj* : sensitive or sensitized to the action of radiant energy
pho·to·sphere \ˈfō-tə-ˌsfir\ *n* : the luminous surface of a star — **pho·to·spher·ic** \ˌfō-tə-ˈsfir-ik, -ˈsfer-\ *adj*
pho·to·syn·the·sis \ˌfō-tō-ˈsin-thə-səs\ *n* : the process by which chlorophyll-containing plants make carbohydrates from water and from carbon dioxide in the air in the presence of light — **pho·to·syn·the·size** \-ˌsīz\ *vb* — **pho·to·syn·thet·ic** \-sin-ˈthe-tik\ *adj*
phr *abbr* phrase
¹phrase \ˈfrāz\ *n* **1** : a brief expression **2** : a group of two or more grammatically related words that form a sense unit expressing a thought
²phrase *vb* **phrased; phras·ing** : to express in words
phrase·ol·o·gy \ˌfrā-zē-ˈä-lə-jē\ *n, pl* **-gies** : a manner of phrasing : STYLE
phras·ing *n* : style of expression
phre·net·ic *archaic var of* FRENETIC
phren·ic \ˈfre-nik\ *adj* : of or relating to the diaphragm ⟨~ nerves⟩
phre·nol·o·gy \fri-ˈnä-lə-jē\ *n* : the study of the conformation of the skull based on the belief that it indicates mental faculties and character traits
phy·lac·tery \fə-ˈlak-tə-rē\ *n, pl* **-ter·ies** **1** : one of two small square leather boxes containing slips inscribed with scripture passages and traditionally worn on the left arm and forehead by Jewish men during morning weekday prayers **2** : AMULET
phy·lum \ˈfī-ləm\ *n, pl* **phy·la** \-lə\ [NL, fr. Gk *phylon* tribe, race] : a major category in biological classification esp. of animals that ranks above the class and below the kingdom; *also* : a group (as of people) apparently of common origin
phys *abbr* **1** physical **2** physics
¹phys·ic \ˈfi-zik\ *n* **1** : the profession of medicine **2** : MEDICINE; *esp* : PURGATIVE
²physic *vb* **phys·icked; phys·ick·ing** : PURGE 2
¹phys·i·cal \ˈfi-zi-kəl\ *adj* **1** : of or relating to nature or the laws of nature **2** : material as opposed to mental or spiritual **3** : of, relating to, or produced by the forces and operations of physics **4** : of or relating to the body — **phys·i·cal·ly** \-k(ə-)lē\ *adv*
²physical *n* : PHYSICAL EXAMINATION
physical education *n* : instruction in the development and care of the body ranging from simple calisthenics to training in hygiene, gymnastics, and the performance and management of athletic games
physical examination *n* : an examination of the bodily functions and condition of an individual
phys·i·cal·ize \ˈfi-zə-kə-ˌlīz\ *vb* **-ized; -iz·ing** : to give physical form or expression to
physical science *n* : any of the sciences (as physics and astronomy) that deal primarily with nonliving materials — **physical scientist** *n*
physical therapy *n* : the treatment of disease by physical and mechanical means (as massage, exercise, water, or heat) — **physical therapist** *n*
phy·si·cian \fə-ˈzi-shən\ *n* : a doctor of medicine
physician's assistant *n* : a person certified to provide basic medical care usu. under a licensed physician's supervision
phys·i·cist \ˈfi-zə-sist\ *n* : a scientist who specializes in physics
phys·ics \ˈfi-ziks\ *n* [L *physica*, pl., natural sciences, fr. Gk *physika*, fr. *physis* growth, nature, fr. *phyein* to bring forth] **1** : the science of matter and energy and their interactions **2** : the physical properties and composition of something
phys·i·og·no·my \ˌfi-zē-ˈä-nə-mē\ *n, pl* **-mies** : facial appearance esp. as a reflection of inner character
phys·i·og·ra·phy \ˌfi-zē-ˈä-grə-fē\ *n* : geography dealing with physical features of the earth — **phys·io·graph·ic** \ˌfi-zē-ō-ˈgra-fik\ *adj*
phys·i·ol·o·gy \ˌfi-zē-ˈä-lə-jē\ *n* **1** : a branch of biology dealing with the functions and functioning of living matter and organisms **2** : functional processes in an organism or any of its parts — **phys·i·o·log·i·cal** \-zē-ə-ˈlä-ji-kəl\ *or* **phys·i·o·log·ic** \-jik\ *adj* — **phys·i·o·log·i·cal·ly** \-ji-k(ə-)lē\ *adv* — **phys·i·ol·o·gist** \-zē-ˈä-lə-jist\ *n*
phys·io·ther·a·py \ˌfi-zē-ō-ˈther-ə-pē\ *n* : PHYSICAL THERAPY — **phys·io·ther·a·pist** \-pist\ *n*
phy·sique \fə-ˈzēk\ *n* : the build of a person's body : bodily constitution
phy·to·chem·i·cal \ˌfī-tō-ˈke-mi-kəl\ *n* : a chemical compound occurring naturally in plants
phy·to·plank·ton \ˈfī-tō-ˌplaŋk-tən\ *n* : plant life of the plankton
pi \ˈpī\ *n, pl* **pis** \ˈpīz\ **1** : the 16th letter of the Greek alphabet — Π or π **2** : the symbol π denoting the ratio of the circumference of a circle to its diameter; *also* : the ratio itself equal to approximately 3.1416
PI *abbr* private investigator
pi·a·nis·si·mo \ˌpē-ə-ˈni-sə-ˌmō\ *adv or adj* : very softly — used as a direction in music
pi·a·nist \pē-ˈa-nist, ˈpē-ə-\ *n* : a person who plays the piano
¹pi·a·no \pē-ˈä-nō\ *adv or adj* : SOFTLY — used as a direction in music
²piano \pē-ˈa-nō\ *n, pl* **pianos** [It, short for *pianoforte*, fr. *gravicembalo col piano e forte*, lit., harpsichord with soft and loud; fr. the fact that its tones could be varied in loudness] : a musical instrument having steel strings sounded by felt-covered hammers operated from a keyboard
pi·ano·forte \pē-ˌa-nō-ˈfôr-ˌtā, -tē; pē-ˈa-nə-ˌfôrt\ *n* : PIANO
pi·as·tre *also* **pi·as·ter** \pē-ˈas-tər\ *n* — see *pound* at MONEY table
pi·az·za \pē-ˈa-zə, *esp for 1* -ˈat-sə\ *n, pl* **piazzas** *or* **pi·az·ze** \-ˈat-(ˌ)sā, -ˈät-\ [It, fr. L *platea* broad street] **1** : an open square esp. in an Italian town **2** : a long hall with an arched roof **3** *dial* : VERANDA, PORCH
pi·broch \ˈpē-ˌbräk\ *n* : a set of variations for the bagpipe
pic \ˈpik\ *n, pl* **pics** *or* **pix** \ˈpiks\ **1** : PHOTOGRAPH **2** : MOTION PICTURE

Exhibit E

IN THE CIRCUIT COURT OF THE
TWENTY-THIRD JUDICIAL CIRCUIT
DEKALB COUNTY, CHANCERY DIVISION

BRENT CAMERON, Individually, and on behalf of all others similarly situated,	)	
Plaintiffs,	)	
vs.	)	No. 2019-CH-000013
POLAR TECH INDUSTRIES, INC., and ADP LLC,	)	
Defendants.	)	

TRANSCRIPT OF PROCEEDINGS at the hearing of the above-entitled cause before THE HONORABLE BRADLEY WALLER, Judge of said Court, in Room 300 of the Dekalb County Courthouse, 133 West State Street, Sycamore, Illinois, on August 23, 2019, at the hour of 10:00 a.m.

REPORTED BY: Nohemi Salazar-Pitts, CSR
LICENSE NO.: 084-4648

APPEARANCES:

STEPHAN ZOURAS, LLP, by
MS. HALEY R. JENKINS and
MR. RYAN F. STEPHAN
100 N Riverside Plaza
Suite 2150
Chicago, Illinois 60606
(312) 233-1550
hjenkins@stephanzouras.com
rstephan@stephanzouras.com

Appeared on behalf of the
Plaintiff and the Putative Class;

JENNER & BLOCK, LLP, by
MR. DAVID C. LAYDEN
353 North Clark Street
Chicago, Illinois 60654-3456
312.922.9350
dlayden@jenner.com

Appeared on behalf of the
Defendant ADP LLC;

O'HAGAN MEYER, by
MR. THOMAS BOWERS
One East Wacker Drive
Suite 3400
Chicago, Illinois 60601
312.422.6100
tbowers@ohaganmeyer.com

Appeared on behalf of Defendant
Polar Tech Industries, Inc.

THE COURT: All right.

THE CLERK: Cameron v Polar Tech.

THE COURT: Do you want to stay there? You don't have to.

MR. LAYDEN: Whatever you prefer, your Honor.

THE COURT: As long as you speak up, I have no problem if you'd like to stay right there.

I'd like you to identify yourselves from my left to my right, please.

MR. BOWERS: Thomas Bowers on behalf of Polar Tech.

MR. LAYDEN: Good morning, your Honor. David Layden on behalf of ADP.

MS. JENKINS: Haley Jenkins on behalf of the Plaintiffs.

MR. STEPHAN: Good morning, Judge. Ryan Stephan on behalf of Plaintiffs.

THE COURT: Did you have something you wanted to tender to me?

MR. LAYDEN: No, your Honor. If you prefer that we step up, we're happy to do it. Whatever you'd like us to do.

THE COURT: Whatever you guys want to do.

If you want to have a seat and argue from there, that's perfectly fine. All right?

So what's before the court is motions to dismiss. Polar Tech has brought a motion under 2-619.1, which, we all know, is a dual motion including 615 and 619. Essentially, their motion is predicated under (a)(5) statute of limitations issue as well as long as (a)(9), and then ADP has filed a 2-615 motion. There is joint response filed by the Plaintiff. There's respective replies. I have had the opportunity to review everything.

Who would like to go first on the Defendants' side?

MR. LAYDEN: Your Honor --

THE COURT: And you can have a seat, by the way. You don't have to stand. Thank you.

MR. LAYDEN: Your Honor, we flipped a coin, and I will go first.

THE COURT: All right.

MR. LAYDEN: Your Honor, as -- and I will obviously repeat a little bit just to try to summarize the high points. ADP's motion first, of all directed, at the Section 15(b) claim of BIPA,

which is the portion of BIPA which requires that an entity collecting biometric information covered by the statute provide written notice and consent and obtain written consent or written release.

Your Honor, the basis for our motion is that the way that the plain language of the statute is structured, you read the entire statute, you focus on 15(b), is that 15(b) applies only to the entity, we think, collecting the data. This is not applied to any entity that is in possession of the data.

And our position is in this case the Plaintiff has alleged, and it's practically Plaintiff's employer, Polar Tech, which actually collected the data. And obviously the employer had control of the workplace, which required that its employees use the biometric and therefore is the collector.

We certainly, of course, as we indicate, don't think it is a valid claim against Polar Tech, but we do believe that if anyone is subject to 15(b), it would be Polar Tech. We think that that is clear from the plain language of statute.

It's also important, Judge, to focus on the definition of "written release," which is set forth in BIPA, which provides that a written release in the context of employment is a release executed as a condition of employment.

And we think, your Honor, that that further affirms our reading of the statute, which is that when you have an employer using biometric technology in the workplace that is covered by the statute, that it is the employer's job to obtain and to provide written notice to get the consent.

Plaintiff's position as set forth in their response is basically that any entity that comes into possession of biometric data at any point in time is subject to 15(b). We don't think that's right, your Honor, because, first of all, it would serve to destroy the careful distinction that the general assembly made in using words like "collect" versus "possess."

If that's really what the legislature intended, they would have just simply said "any entity coming into possession of biometric data needs to get notice and get consent." That's not what the legislation said, and we think that's

very important to recognize.

The Plaintiffs also focused on the word "obtain," or actually it said the words "otherwise obtain" at the end of 15(b), and suggested that that's essentially just akin to coming into possession. We don't agree with them, first of all, in line with what I just said, which is that it would collapse the distinction that the legislature made.

And second of all, the word "otherwise obtain" comes at the end of a string of other words, "capture," "collect," which all involve, essentially, an active process of obtaining information from the actual individual who has the biometric data, and therefore we think that it needs to be read consistently with that, meaning an interaction with the person who has the biometric data and the opportunity to give notice and obtain release, if that is required.

And for all those reasons, we don't believe that the 15(b) claim can stand. And if you look at the complaint, your Honor, it's pretty clear that the specific allegations in the complaint are that Polar Tech was the entity

collecting.

Certainly, the Plaintiff has included some general allegations that each Defendant or that Defendants actively collected. But I think if you look at the Plaintiff's theory of the case is that Polar Tech used the clock in the workplace to obtain the employees' biometric information and then it was later, according to Plaintiffs, disclosed to ADP, meaning that ADP was not collecting; ADP was receiving it afterwards. That's the theory that we believe is set forth in the complaint. And we believe that that forecloses the Plaintiff from a pleading, a claim, against ADP under Section 15(b).

We also would move to dismiss the Section 15(a) claim, your Honor, and that is the one that requires an entity in possession of biometric information covered by the statute to develop a written retention policy.

Your Honor, as we have set forth in our brief, the Plaintiff had argued initially that ADP violated it by not providing the policy to Plaintiff. That's not what the statute requires. The Plaintiff seems to have now backed off a

little bit and said we have to have a policy. And, your Honor, first of all, that's not what the statute requires. The statute actually has different language. It says you must develop, which to us means plainly that when you come into possession of biometric information, you then must develop a policy.

And I think just to be clear here, your Honor -- and we haven't raised a 619 motion, so this may have to be a summary judgment issue if we don't prevail today on this. But ADP had a biometric policy in effect in October 2017. The Plaintiff started working in early 2018, so there is not going to be a Section 15(a) claim against ADP unless the Plaintiff is going to challenge the efficacy of the policy. I don't understand them doing so, but we may have to get to that.

So we think that the 15(a) claim fails to state a claim because they just haven't alleged that ADP violated that section of BIPA.

And then, your Honor, finally, that leaves us with the alleged claim under 15(d), which is the section of BIPA that deals with disclosure/disseminations. And here what we

really have is a very conclusory obligation.

In parts of their Complaint, the Plaintiff alleges that Polar Tech has collected and then disclosed to ADP. But then they say, well, ADP also disclosed to cloud storage providers and other vendors. It's actually not true, but for purposes of their pleading, our position is that they haven't pled that that's the issue.

THE COURT: Can I ask you a question?

MR. LAYDEN: Certainly, your Honor.

THE COURT: My understanding is that you concede in your, I think it's your reply, I could be wrong, that there was a -- it was transmitted to a third-party storage provider.

MR. LAYDEN: Your Honor, I don't think we did, and if we did, we misspoke, and so I apologize for that. I can tell you also --

THE COURT: I want to be accurate.

MR. LAYDEN: Sure. Of course. I can tell you, and I realize that we're stepping a little bit outside pleadings, your Honor; but ADP does not disclose or give data to anyone else. The data -- any data that ADP gets stays at ADP.

Plaintiffs, obviously, are entitled to allege that, but I just -- I'm telling you what the facts will ultimately show.

THE COURT: Just give me a moment because I do not want to state something that is inaccurate.

It must have been with the -- I apologize. It must have been what the Plaintiff had alleged, because I'm looking at your reply and I do not see it in here. As a matter of fact, you can test that.

So go ahead.

MR. LAYDEN: Very well, your Honor. So basically the -- so putting aside what actually happened, because I appreciate in the 615 motion, you need to deal with the specific facts alleged. We understand that. There is no -- there are no specific facts alleged as to a disclosure/dissemination.

And even if -- this is obviously assuming, because it's not true. Even if they could allege that ADP had disseminated it to a cloud storage provider, our view is that is not a disclosure/dissemination because -- for two

reasons: A, the dictionary definition of disclosure or disseminating would mean essentially to reveal something. It's to reveal to someone who does not have a right to have it.

And the cloud storage provider simply provided, essentially, an administrative service, and it would be a significant expansion of BIPA to say that any time a cloud storage provider is ever provided data that there needs to be, essentially, disclosure consent.

And, actually, taking Plaintiff's theory to the actual logical conclusion, I think they would say that 15(b) applies to cloud storage providers. So if anyone ever were to switch storage providers, they would have to somehow get back and go to all the people who they collected data from and get that information including former employees. So I think it becomes one whirlpool very, very quickly.

So, your Honor, we're not contending that, you know -- as Plaintiff said that, you know, that ADP could do whatever they want with this data, but they can't give it to -- you know, they can't sell it, they can't provide it to

people who -- for purposes other than what it has been collected for.

But even assuming -- again, it's not true, but even assuming ADP had used a cloud storage provider, we don't believe that it constitutes a disclosure or dissemination under the statute.

As a matter of fact, it is in Section 15(b) of the statute, a provision talks about what happens when you transmit data and how you have to deal with it when you transmit it, and then if you transmit it, you're not allowed to disclose it, which to us is further confirmation that not every transmission of data to someone else constitutes disclosure, because otherwise that section doesn't make any sense.

So, your Honor, for those reasons -- and I'm obviously happy to answer any further questions you have -- we don't believe that the complaint alleges a sufficient claim under BIPA against ADP, and we would ask that it be dismissed with prejudice.

THE COURT: And you're also moving to dismiss the common law negligence count as well,

correct?

MR. LAYDEN: Your Honor, we are. And obviously Plaintiff's counsel can address this. I don't understand they're proceeding on that, at least in other cases they have dropped that claim post Rosenbach. But we are -- to the extent they are proceeding on that, we are, in fact, proposing it for the reasons that we have said at this time.

THE COURT: And you are also saying that the statute of limitations issue which was raised by the co-Defendant is premature at this point because the named Plaintiff, whether you pick the one-, two-, five-year statute of limitation, was filed, even in the worst case, within the one-year statute of limitations; is that correct.

MR. LAYDEN: Your Honor, that is ADP's view. I don't want to step on Polar Tech's toes.

THE COURT: I'm not -- no. I'm the one bringing it up, so you're not stepping on their toes.

MR. LAYDEN: You're right. That is what we believe to be the case. But obviously Polar Tech has a relationship with the Plaintiff, and they are aware, obviously, of the facts relating

to his employment status. So we are just not in the position to say that, but based on the briefs, that is what we believe.

THE COURT: Okay. Very good.

All right. The way I'm going to handle this is that I'm going to allow you to respond to ADP, and then you get the last word on your motion, and then we will move to Polar Tech.

You're up.

MS. JENKINS: Thank you, your Honor. ADP is essentially claiming that only certain sections of BIPA don't apply to it, but the plain language of the statute makes clear that it applies to all private entities that come into possession or that obtained this data, and to private entities as defined by the statute.

THE COURT: Can I ask you this question? What data is ADP actually acquiring?

MS. JENKINS: Well, your Honor, ADP is the manufacturer of the clock, the manufacturer of the software, and is additionally supporting the services, and they're obtaining whatever data that clock is taking from the Plaintiff. So when he puts his fingerprint on the clock and it takes

that fingerprint data from him, that's the data that they're obtaining.

THE COURT: Okay. But -- and I know a little bit about this, I think, but, I mean, there's different ways to obtain data. So you can have the data that I think is contemplated by the statute which is that you have somebody's biometric information in the form of a fingerprint or a retina scan, et cetera, as defined, or you can have data that -- I don't know if you're familiar with the terminology of a hash function where a hash function is essentially, as I have always looked at it as, is it's kind of like gibberish, it's encrypted, it's something that -- it's like, you know, your password.

So if you type in your password, you know, "I love mom," the hash function recognizes that, but it doesn't recognize it word-for-word. So it seems to me it begs the first question: What data, in your view, is ADP actually acquiring from your client?

MS. JENKINS: Well, your Honor, the first part is that they may be acquiring his actual biometric identifier, his actual fingerprint; but

the statute also contemplates biometric information, which is any information derived from that fingerprint.

So even if -- and I'm going to anticipate ADP would argue that they're collecting some encrypted mathematical template of his -- of the fingerprint scan the Plaintiff puts on the time clock. But that is biometric information, and that is data that they're collecting.

THE COURT: So you think the statute is broad enough to encompass and include encrypted or hash functions?

MS. JENKINS: I do.

THE COURT: Go ahead.

MR. STEPHAN: And, Judge, if I can add one thing on that.

THE COURT: Yes.

MR. STEPHAN: And this is sort of how computers work, right? If you look at any image on your computer, there are numbers behind it. That's how the computers communicate. So they don't -- it's not like a hard copy fingerprint that you would see at a police office. So it's how computers communicate, and we clearly believe

that's contemplated by the statute.

THE COURT: But, to your point, they communicate by use of digits, they communicate by use of codes. So, you know, you could look at the data collected by virtue of the fingerprint or the retina scan and have absolutely no idea what you're looking at.

You believe that's contemplated by the statute?

MR. STEPHAN: Well, I don't believe that your first part of that is necessarily accurate. Anything that is encrypted can be unencrypted, and oftentimes numbers represent other things. So we do feel like that is included by the statute and we feel that it is under the definition of biometric information covered by the statute.

THE COURT: What section would you direct my attention to, of the statute?

MS. JENKINS: In Section 14/10 is the definition of biometric information.

THE COURT: So your position is biometric -- the biometric identifier and the biometric information, those two coupled together would include encrypted/unencrypted, hash

functions, et cetera?

MS. JENKINS: Yes.

THE COURT: And your position would be under biometric information means any information regardless of how it's been captured, converted, stored, or shared?

MS. JENKINS: Exactly.

THE COURT: Go ahead. By the way, do you have the case on that?

MS. JENKINS: I'm sorry?

THE COURT: Do you have a case or cases on that?

MS. JENKINS: Not yet. It's still being litigated.

But, your Honor --

THE COURT: I don't ask questions I don't know answers to, but ahead.

MS. JENKINS: So, your Honor, I think one of the important things to remember is that ADP bases its entire business model on the fact that it's collecting this data, sets out to collect this data because it creates the time clocks that do it and software that goes along with it. It integrates those programs into it's various HR and

payroll functions that it provides to various employers, and it profits from all of this.

So to call them not a collector of the data, we just think would simply inaccurate. It's actually one of the biggest collectors of this type of data, which means it should be the most knowledgeable in this space, the most experienced. It's one of the most vulnerable if attacked, and it's the most culpable here as well. And yet they did nothing absolutely to comply with BIPA.

We are at a Section 2-615 motion to dismiss stage, and if you look simply at the pleadings with respect to Section 15(a), we allege, and ADP hasn't really disputed that they possessed the Plaintiff's biometric data.

We alleged that they didn't have a written publically available retention and destruction policy, and if discovery bears out that they might have produced that prior to the Plaintiff's employment, so be it, but we are talking about the allegations in the pleadings right now; and under the pleadings and within the boundaries of the complaint, we have properly

alleged a claim with respect to 15(a).

With respect to Section 15(b), we have alleged, and they don't really dispute it, that they failed to provide the requisite notice under BIPA and they failed to obtain a written release from our client, all before collecting his biometric data. Instead, they just want to write themselves out of the statute, but as we stated before, Section 15(b) applies uniformly to all private entities that collect, capture, or otherwise obtain this data.

THE COURT: How would ADP have any sort of privity or the ability to effectuate the elements under B? In other words, it talks about that has to be obtained before the collection of the data, correct? So how would they be in a position to do that?

MS. JENKINS: They could easily implement on their own device, you know, a pop-up screen that comes up when the Plaintiff or another individual first uses the device that says, you know -- it has BIPA-compliant written disclosure and asks for their written consent to do so.

They could also require their

customers, the employers, to include them on any BIPA-complaint disclosure and a release that they provide to their employees prior to collecting the data.

There are a number of ways that they could comply with the statute, but they have chosen not to. They then want the Court to believe that collection rests only with the employer, but this position just simply makes no sense.

That would be like saying, when the minister passes around the collection plate at church, only the minister is collecting the money and not the church, and we all know that that's not true; and that's not how data works in our day-to-day lives either. It doesn't stay with the initial collector. No data that you provide to one, you know, company or to one venue generally stays with that. It's disseminated across several platforms and integrated into other platforms, as ADP well knows.

And with respect, again, to Section 15(d), we have alleged that they had disclosed or disseminated the Plaintiff's

biometric data to third parties. And the biggest contention is that the conclusions -- or their allegations are conclusory, but we can't be expected to know at the pleading stage where everything that they have disclosed has gone and who it's gone to.

But we do know from our own investigation and from our experience in this field that the data is shared or at least able to be accessed across a number of different platforms by a number of different parties.

Again, if discovery bears out that an allegation turns out not to be fruitful, that's an issue for a different time. Based on the pleadings we have alleged that ADP violated Section 15(d). ADP also claims that Section 15(d) requires some sort of public disclosure of Plaintiff's data, but the plain text of BIPA does not require that. It just requires that it be disseminated or disclosed to a third party.

You could disclose something to a third party without making it known to the public at large, which is what we have alleged that they have done here.

So, again, your Honor, I think it's important to consider that we're still at the pleading stage, and based on the allegations in the Complaint the Plaintiff has properly alleged the violations of Sections 15(a), (b), and (d) of BIPA with respect to ADP.

THE COURT: Anything else?

MS. JENKINS: Not unless you have questions.

THE COURT: Do you have anything?

MR. STEPHAN: No, Judge. Thank you.

THE COURT: Okay. You get the last word. It's your motion.

MR. LAYDEN: Thank you, Judge.

So just to re-respond, and actually -- well, to your questions and also to what Plaintiff's counsel said; first of all, the way the technology works, there is no fingerprint involved. The scanning function essentially measures -- it's much, much less precise than a law enforcement fingerprint, so anything that you may have seen on TV or what we think of as actual fingerprints, it's not involved here.

The scanning essentially measures a

few points on the fingertip, on a portion of the fingertip. It then creates this mathematical template that your Honor referenced; it's encrypted, it's just a series of hexadecimal numbers. That's all that it is. There's no fingerprint stored, there's no image of the fingerprint stored. It's just a series of numbers. So that's what we're dealing with here.

And, your Honor, we certainly disagree, and I think I may have previewed this a little bit in my opening remarks. We don't believe this technology is covered by the statute. We do believe, though, that there probably is going to be summary judgment issues as opposed to a -- or maybe a trial issue as opposed to a motion to dismiss issue.

So we're not at all conceding that it's covered, and, your Honor, I think your question goes to one of the key arguments we're to be raising, which is it just simply isn't covered.

A couple of other points just to respond to what Plaintiff's counsel said, it's actually not true that ADP manufactures the clocks. ADP doesn't. ADP buys the clocks from a

company called Kronos that actually manufactures them. And that's important, your Honor, because it goes to something else that Ms. Jenkins said.

Your Honor asked whether -- how could ADP have actually obtain, provide notice and get consent, and that's obviously going to be focused on our briefs. And one of the suggestions that Plaintiff's counsel has alleged is we could just build it in the clock software. Well, that's impossible, your Honor. We don't write the clock software; it's Kronos software.

So you're essentially suggesting that something that we buy from someone else, we should somehow be required under BIPA to reprogram, which we can't because we don't actually have the source code to provide this onscreen notice.

And then the other suggestion Ms. Jenkins made was that we could just rely upon the customers to provide notice and get consent. Well, actually, the problem with that, your Honor, is that BIPA has these $1,000, $5,000 per item penalties, and that's a significant risk to ask a company like ADP to run because certainly we would expect that all of our clients would comply with

the law in every instance.

But when we have the plaintiffs all over this country who are filing these lawsuits by the dozens and hundreds, and so basically for their end, for their response that they make repeatedly, well, you can't just rely upon someone else to take care -- or just rely upon someone else to just take care of any financial liability. We don't think it's workable, and frankly it's not what the statute says, your Honor. The statute says that -- it talks about a collector, it talks about the companies that may become in possession.

And, your Honor, Ms. Jenkins' used an interesting analogy, the minister with the collection plate, which is not one I have heard before, but I actually certainly think it is pretty interesting.

THE COURT: Well, we have ushers in my church who pass the plate.

MR. LAYDEN: Yeah, I was going to say that, but I thought they were ushers, and the minister is not going to have much to do with the ushers just passing it around.

But I think actually the analogy

works a little bit better if you think about it this way: The minister, or the church, is Polar Tech; the people passing around the collections plate are the supervisors. They are folks in Polar Tech's facility who are in charge of making sure its employees use these clocks to clock in and out of work so they can be paid wages by Polar Tech in connection with their employment of Polar Tech.

I don't think it would be reasonable for the Plaintiff to sue all those supervisors individually and say that they were collecting, and try to subject them to 1,000 liability. Instead, I think that the way BIPA works is that the entity that is actually collecting the data for use in its business, which is the employer, is the entity that is the collector, it's not the supervisor, it's not someone like that.

So I think actually that analogy does work if you just switch the entities out a little bit. I think that the ushers are the supervisors.

So, your Honor, I think for all those reasons, you know, I think that the Plaintiff's response doesn't really quite meet the arguments

that we made in the brief. I think that this is a situation where understandably they're really trying to stretch BIPA way beyond its limits in terms of who is covered by this, and I really think that it just creates a real practical problem.

We should not be construing laws in ways that make it impractical or impossible for entities to comply, particularly where you have such a draconian penalty scheme in it. And that's really what they're asking for, and it's really kind of a trap for companies like ADP which are marketed for selling its clocks, providing its services.

So for those reasons, we don't think there's any basis to apply 15(b) to ADP, and I don't think -- I think that my remarks on 15(a) and 15(d), I think, can stand; and for those reasons, your Honor, we would ask that you grant our motion to dismiss the claims. Thank you.

THE COURT: Thank you. This is a very intriguing area for me. I'm going to deal with the simple thing first or simple count first. I did not see that the Plaintiff gave any sort of a

response to the, what I'll term the common law negligence claim, but to make the record clear, there is a statutory provision that I believe predominates, and I'm going to dismiss the common law negligence claim with prejudice under 619(a)(9).

The -- and that also addresses what Polar Tech raised, but in any event, what's really in play here is the statute, and the statute is the Biometric Information Privacy Act found at 740 ILCS 14/1 at (c), and it addresses a number of issues.

And what, however, is before me today with respect to ADP is a 2-615 motion. And as we all know, 2-615 is the motion under the Code of Civil Procedure that mandates that I look to the four corners of the pleadings and the four corners of the pleadings only, and that's what I have done.

I'm admonished that I'm to construe the complaint in the light most favorable to the nonmoving party. It's what I like to call the "so what" motion. So, what you have alleged does not state a cause of action, in this case under the

statute that's before me.

So diving into this, the complaint -- we're going to start with, since both sides have started with 15(b), I'm going to start there. 15(b) of the statute provides that no private entity, and I really have not heard, nor did I see in any of the briefs, if you will, there's no dispute, there's no contest, there's no argument that ADP is anything but a private entity.

No private entity may collect, capture, purchase, receive through trade or otherwise obtain a person's or a customer's biometric identifier or biometric information unless it first, so in other words, before, it collects, captures, purchases, receives, or otherwise obtains, it first must inform the subject or the subject's legally authorized representative in writing that a biometric identifier or biometric information is being collected or stored;

Two, informs the subject or the subject's legally authorized representative in writing of the specific purpose and length of term for which a biometric identifier or biometric

information is being collected, stored, and used, and receives a written release executed by the subject of the biometric identifier or biometric information or the subject's legally authorized representative.

There's a definition of written release, and that means informed written consent or, in the context of employment, a release executed by an employee as condition of employment. Although not really addressed in any of the briefs, the issue of what is a -- or what's the definition of a legally authorized representative. That's not set forth in the statute. Does that mean the employer? There are no cases that interpret that.

So I have to give effect to the plain language of a statute. I'm mandated by the Appellate and Supreme Court to do that. And the best way is to look at the plain language and not to excise out a particular section, but to read the statute in its totality.

So it seems to me that trying to give effect to the statute as a whole where a cause of action would accrue would really be under 15(a),

(b), (c), (d), and (e), as to what, if you will, a private entity can do with the data as defined in the statute. So to try to give effect to the whole of the statute, it's this court's view that 15(b) only applies to an employer and not a third party.

It seems to me that trying to give effect to this, the information is, first and foremost, it is a before, unless it first informs the subject or the subject's legally authorized representative. And if I look at the pleading, it seems to me that the intent of this section is for an employer to be, if you will, responsible for providing that information. And I'm trying to give effect to the definition of written release in the employment context, and that by its plain language states that.

So I always hate to be on the cutting edge because that branch can get real thin real quick, but unfortunately I don't see a case that is directly on point interpreting this. The statute is fairly new, as we all know, but my view is that it applies when it is an employment situation, which is the allegation here, that it's

the employer's responsibility, not a third party, and I'm going to grant the 2-615 motion with respect to 15(b), with prejudice.

15(a) does not require that a private entity provide an individual with anything. It is -- what it states specifically, for the record, is that a private entity in possession of biometric identifiers or biometric information must develop a written policy made available to the public establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information, and it goes on. I don't think I need to go any further.

But with respect to the pleadings, I think there needs to be more specificity than just a recitation of the statute. But I don't think the pleadings correctly or accurately state that, and I'm directing everyone's attention to paragraph 44, "Furthermore, each defendant fails to provide employees," that's not required, but I am certainly going to give, with respect to a 15(a) allegation, the Plaintiff the opportunity to replead. So the 615 motion will be granted, however, it will be granted without prejudice.

15(d), this is interesting. 15(d) provides that "no private entity in possession of a biometric identifier or biometric information may disclose, re-disclose or otherwise disseminate a person's or a customer's biometric identifier or biometric information, unless the subject of the biometric identifier or biometric information or the subject's legally authorized representative -- there is it is again" -- "consents to the disclosure or re-disclosure, the disclosure or re-disclosure completes a financial transaction requested or authorized by the subject, the biometric identifier, or the biometric information, or the subject's legally authorized representative --" it's not applicable here -- "the disclosure or re-disclosure is required by State or Federal Law or municipal ordinance, or the disclosure is required pursuant to a valid warrant or subpoena issued by a court of competent jurisdiction."

But what's in play here is no private entity in possession of a biometric identifier or biometric information may disclose re-disclose or otherwise disseminate. With respect to again, the

four corners of the pleadings, it seems to me that there are not sufficient facts, there's not sufficient specificity just to say it was disclosed without more.

And, again, like I did under (a), I'm going to grant the motion; however, it's going to be without prejudice to replead. And so that will be the order of the Court with respect to ADP's motion.

You're up.

MR. BOWERS: Thank you, your Honor. And I apologize, I'm also getting over a cold, so I'll do my best to speak up.

THE COURT: No apologies necessary.

Go ahead.

MR. BOWERS: So given the fact that your Honor has already addressed Polar Tech's argument with respect to Plaintiff's Common Law negligence claim, I'll just start turn my attention to the statute of limitations issue that's before you.

We filed a Section 619 motion with respect to the statute of limitations --

THE COURT: (a)(5)?

MR. BOWERS: Correct, (a)(5)motion.

As your Honor is well aware, BIPA does not contain an expressed statute of limitations. This is an area that's being litigated amongst circuit courts across Illinois, and these lawsuits continue to be filed by plaintiffs' attorneys in Northern Illinois and across the state.

It is Polar Tech's stance that a one-year statute of limitations applies to Mr. Cameron's BIPA claim because BIPA is a statute that is concerned with the right of privacy and the protection of privacy rights.

Alternatively, Polar Tech submits that in the event a one-year statute of limitations does not apply, a two-year statute of limitations applies to limit any claims of the Plaintiffs and/or the putative class to two years arising two years before the date of filing the complaint, which in this case would be August 7th of 2016.

Based on the fact that the Illinois Supreme Court's decision in Rosenbach v Six Flags effectively transformed BIPA into not only a strict liability statute, but also a penal

statute, as opposed to a remedial statute, as Plaintiff asserts in his response brief.

With respect to Polar Tech's assertion that a one-year statute of limitation applies -- this falls under Section 13-201 of the Code of Civil Procedure, a one-year statute of limitation applies in the event that there is a publication --

THE REPORTER: Your Honor, I need him to speak up.

THE COURT: Can you speak up a little bit for the court reporter.

MR. BOWERS: Yes. Sorry.

A one-year statute of limitation applies to privacy claims in the event that there is publication of the information that was, in this case, purportedly collected, stored and, as alleged in Plaintiff's, disseminated.

In Plaintiff's Complaint, there are allegations that biometric data was not only collected and stored, but also disseminated to third parties, ADP, and, quote, "other unknown third parties."

There is a case out of the First

District Appellate Court called Popko v Continental Casualty Company. That cite is 355 Ill. App. 3d 257. It's a 2005 case out of the First District. In that case, an employee was terminated from CNA Insurance, Continental Casualty Insurance.

After undergoing a performance review in which he allegedly used profanity during this performance review with his supervisor. That supervisor sent a memorandum to yet another supervisor, a manager within the company, and the plaintiff was ultimately terminated in that case.

And in that case he brought a defamation claim against his former employer, but the focus of the court's opinion there was whether or not there was publication. And I bring this particular case up, not for the defamation part of the case, but to address the issue of publication.

In that case, the court said that there was publication solely by virtue of the fact that information regarding the plaintiff's performance review was transmitted by his supervisor who was present at that performance review to another individual within the company.

So in that case, an intra-office communication from one individual to another, while not made directly available to the public at large, can constitute a publication.

And similarly here, that's what's been alleged in Plaintiff's Complaint. Plaintiff has alleged that Polar Tech collected and stored Mr. Cameron's biometric data by virtue of his usage of providing scans of his finger on a time clock system that was provided by ADP, and that that information was then disseminated to a third party, in this case ADP, and potentially to other third parties.

BIPA itself is concerned with publication, as seen in Section 15(c) and section 15(d).

THE COURT: Can I stop and ask you a question?

MR. BOWERS: Sure.

THE COURT: So the allegations in the Complaint is that the Plaintiff was employed by your client from February of 2018 until May of 2018, and this is a 619, so you admit all well pled facts. And this case was filed on 8/7 of

'18. So would I be correct in assuming that what you're directing my attention to would be the class action component of this pleading?

MR. BOWERS: That's correct.

THE COURT: Go ahead.

MR. BOWERS: So, yes, we are directing your attention to the class action component for this particular claim as opposed to Mr. Cameron's actual dates of employment. But as stated before, BIPA does concern itself with publication in Sections 15(c) and 15(d).

THE COURT: But you would agree that, I mean, the Complaint was filed even in the shortest statute of limitation, which is a year that you're asking me to consider, right?

MR. BOWERS: Correct.

THE COURT: Okay. Go ahead.

MR. BOWERS: I will concede the fact that this complaint was filed within one year of Mr. Cameron's employment.

THE COURT: Okay.

MR. BOWERS: But for purposes of the class size, that will be determined down the road. That's why I preface it now, because I don't want

to waive this argument later.

THE COURT: I understand.

MR. BOWERS: BIPA does prohibit parties from selling and trading or profiting by dissemination of a person's biometric data and also prohibits parties from disclosing re-disclosing, or otherwise disseminating an individual's biometric data, and this signals the Illinois General Assembly's intent to regulate dissemination and, therefore, publication of an individual's biometric data to third parties.

Again, publication is not required, that this data be made available to the public at large, or that could be made available to the public at large, it requires that it's transmitted to a third party. Because Illinois takes a more narrow view of what "publication" means as opposed to other jurisdictions in this country.

So, accordingly, we submit that a one-year statute of limitations applies to Mr. Cameron's claim.

Alternatively, if the Court is inclined that to opine that the one-year statute of limitations does not apply, Polar Tech submits

that a two-year statute of limitations applies, because Mr. Cameron seeks a statutory penalty in its prayer for relief.

BIPA provides liquidated damages of $1,000 per negligent violation, and $5,000 for intention and/or reckless violation of the Act.

Plaintiff asserts that a five-year statute of limitations applies to his claim because BIPA does not contain an expressed statute of limitations. And while BIPA itself does not contain a specific statute of limitations, unless a rule to the contrary applies, then the five-year statute of limitations, the catch-all provision, applies. And that's exactly what that is, a catch-all, a backup, if nothing else applies.

Here alternatively, a two-year statute of limitations would apply should the one-year statute of limitations not apply, because the Supreme Court's decision in Rosenbach v Six Flags not only transforms BIPA into a strict liability statute, it also rendered it into a penal statute.

A statute is there for penal if it imposes automatic liability or violation of its

own terms, if it sets forth a predetermined amount of damages, and if it imposes liability without actual damages suffered by the plaintiff.

In Rosenbach, the Supreme Court held that the plaintiff did not need to allege actual damages in order to bring a claim underneath the umbrella of the statute. That is exactly what happened here.

Plaintiff then attempts to rebut my argument by saying that BIPA addresses a societal concern, in this case regulating an individual's privacy and their biometric data, which, fine, I will concede that it may have been an intent. But a statute can both be penal and serve remedial purposes.

In Plaintiff's response, they bring up the Telephone Consumer Protection Act, and whether -- in the case called Lay, whether or not that statute was remedial or penal. And in that case, the court noted that the TCPA were provided for treble damages, which were separate from the liquidated damages contained within the statute. That's a distinguishing feature from BIPA.

BIPA does not contain such a

provision. It provides solely liquidated damages. It provides punitive and deterrent goals to prevent abuse of individual -- collection of an individual's biometric data. It is distinguishable from TCPA.

And in the event that a one-year statute of limitations does not apply, because the statute is penal in nature, it has deterrent and punitive goals, it provides a predetermined amount of damages, it imposes liability without regard for actual damages as articulated by the Illinois Supreme Court in Rosenbach, and it imposes automatic liability for a violation of its own terms, which the Illinois Supreme Court rendered the statute into a strict liability statute through Rosenbach.

This statute is penal in nature, not remedial, and alternatively, a two-year statute of limitations would apply to this lawsuit in general, to BIPA claims in general.

THE COURT: Anything else?

MR. BOWERS: That's all I have.

THE COURT: You will get the last word.

MS. JENKINS: Thank you, your Honor.

We would first like to acknowledge we do agree with the court. This isn't properly at issue right now. The Plaintiff's claims were filed within one year, so even assuming the short statute of limitations, this complaint cannot be dismissed on those grounds alone.

Instead, this is Defendant's improper attempt to limit the class size, which it's more properly handled by the motion for class certification or potentially a summary judgment. But regardless, as it's been noted, BIPA has no self-contained statute of limitations, and therefore, the statute of limitations provided by 735 ILCS 5/13-205, which is the default five-year limitations period, should apply.

The one-year statute of limitations does not apply here for two reasons. First, while we might allege that Plaintiff's privacy has been denigrated by virtue of Polar Tech violations of BIPA, the true nature of a potential liability here stems from Polar Tech's violation of the statute itself. This is not an action for slander

or libel or publication of a matter violating the right to privacy.

The plain and unambiguous language of Section 13-201, which provides the one-year statute of limitations states that it applies to actions for publication of a matter violating the right to privacy, which is not what's being alleged here. The defendants in these cases can't have it both ways saying that publication is a necessary element for the statute of limitations, but dissemination only takes place if it's made to the public at large.

The positions that have been taken, and I understand that ADP and Polar Tech were making separate arguments, but these types of positions are inconsistent. And further, the plain and unambiguous language of BIPA doesn't require us to allege publication, and therefore we don't believe that BIPA falls within the one-year statute of limitations period.

Polar Tech, alternatively declares that the two-year statute applies because it thinks that BIPA is a penal statute; but penal statutes impose automatic liability, which BIPA

does not. It sets forth a predetermined amount of damages, and BIPA does contain statutory damages in the event that Plaintiff doesn't recover their actual damages.

They also claim that BIPA imposes damages without regard to the actual damages suffered by the Plaintiff, but that's simply not true. If you read the statute, Section 14/20 provides that a plaintiff can recover actual damages or statutory damages, whichever is greater, and, therefore, BIPA is not a penal statute.

It is analogous to the Telephone Consumer Protection Act, or TCPA, which provides that a plaintiff can recover actual damages or $500 per each violation, whichever is greater. The language is almost the same as the language in BIPA.

And as the Illinois Supreme Court recognized in Standard Mutual Insurance Company v Lay, the TCPA is not a penal statute with that identical statutory language, and therefore BIPA shouldn't be considered one either.

Rosenbach didn't make BIPA a penal

statute. It again reiterates that a plaintiff could recover actual damages if they properly pled and proved them or statutory damages. And they don't need to allege actual damages because the statute provides statutory damages. Therefore, only the five-year statute of limitations remains.

And furthermore, Judge, no case or court or judge has considered this issue, directly or indirectly has adopted the Defendant's position. Every court that has considered this issue has ruled in favor of the five-year statute of limitations. And I recognize that none of those cases are binding on this court, but we do think that they're persuasive in holding that several judges across both the country and the state have held that the five-year statute of limitations applies.

And we filed with the court a notice of supplemental authority. The case Robertson v Hostmark Hospitality Group, which I have copy of if you need it today; and in that case Judge Cohen in Cook County also held that the one-year and two-year statute of limitations do not apply for the reasons we have articulated, and agreed that

the five-year statute of limitations period is not applicable here.

Other cases, in ruling on motions for class certification, have held that the five-year statute of statute of limitations period is applicable with respect to the class size, and those cases are Alvarado v International Laser Production Inc., Case No. 18-cv-07756 in the Northern District of Illinois decided on June 19 of 2019; Roberson v Symphony Post Acute Network, Case No. 17-L-733 in the Circuit Court of St. Clair County, in March of 2019; and the Facebook Biometric Privacy Litigation case pending in the Northern District of California, which was determined and decided in April of 2018.

And for these reasons, we believe that the five-year statute of limitations period is the one that applies to BIPA and not this shorter one or two-year periods.

THE COURT: Thank you.

Last word.

MR. BOWERS: Your Honor, just a couple of things to address, and I'll do my best to make this quick.

First, Ms. Jenkins has stated earlier that the allegations contained in this complaint focused on the violation of the statute based on the collection of biometric data. They have also alleged that this data was disseminated to third parties, and BIPA itself expressly prohibits dissemination and publication of data to third parties.

That is part of the violation of BIPA. There are multiple ways to violate the statute: By profiting, by collecting, by capturing, by storing, by disseminating, by publishing.

Publishing and collecting were both alleged in this complaint. BIPA expressly prohibits publishing and disseminating biometric data to third party. That was what was alleged in this complaint. So, accordingly, we would submit that a one-year statute of limitations does apply to this claim.

Secondly, with respect to the argument of the two-year statute of limitations, as I have stated before, this statute does contain express liquidated damages based on the type of

violation of the statute. It imposes liability automatically for violation of its terms based upon a plain reading and interpretation of the Illinois Supreme Court's decision in Rosenbach.

This statute has been transformed into a strict liability statute, and it has been transformed into a penal statute, and alternatively, a two-year statute of limitations should apply to a BIPA claim.

And, finally, I'll just bring up the authority, the supplemental authority that Ms. Jenkins has just brought to your attention. None of these cases are -- none of these decisions are binding on this court. We have a decision out of the Northern District of Illinois, at a St. Clair County, and out of the Northern District of California. None of those cases, none of those decisions are a binding precedent on this court.

And so accordingly, Polar Tech submits that those decisions should be disregarded as they are not binding on this court.

THE COURT: Thank you.

Excellent job. But as I thought through this, it seems to me that this is

premature. I don't have before me anything more than the complaint which pertains to the named Plaintiff. I understand why you did what you did. You want to preserve this. It is preserved. But I'm going to enter and continue my decision on that until, I don't know, class certification, summary judgment.

But certainly, in my view, the record needs to be developed much more than it is, but Polar Tech is in no way, shape, or form prejudiced, precluded, foreclosed from addressing this as we get further down the road. So I am not ruling on this. I'll enter and continue the issue for a later date.

That being said, how much time does Plaintiff need to replead on the Counts or the sections that I left up?

MS. JENKINS: 30 days, your Honor, if that's okay with you.

THE COURT: That's reasonable. Here's the offer that I will make. Okay? I know this is isn't the only file on your respective desks. I don't believe in bringing back attorneys unless we're going to accomplish something of substance,

so I will throw this out.

I don't know what your respective thoughts are, obviously, because you haven't seen the amended pleading, but I'm affording you ample opportunity to decide whether you're going to file a motion to dismiss; I'm willing to do that.

You're all excellent lawyers. You can work out a briefing schedule. I can give you an outside date right now for a hearing date. If it ends up being that you file an answer, we could just use that as a status date on discovery, et cetera.

Would you like to take me up on my offer.

MR. LAYDEN: It's certainly fine with ADP, your Honor.

THE COURT: Why don't we kick this out for status/argument. How about if we go to the beginning of December? That gives each side a full opportunity to work out a briefing schedule, with the caveat that I get courtesy copies one week before, but I'll just throw out arbitrarily Wednesday, December 4th at 10:00 for argument or status.

MR. LAYDEN: Your Honor, that day is not terrific for me. Any other day that week is fine.

THE COURT: December the 6th? That's a Friday at 10:00.

MR. STEPHAN: Judge, can we suggest maybe pushing that to January. The holidays are just -- I'm always jammed.

THE COURT: I'm not opposed at all. Might I suggest the 17th, 10:00?

MR. LAYDEN: Fine with me.

THE COURT: Argument or status?

MR. BOWERS: Judge, I'm scheduled to be out of town that day. Is there a day that week, maybe earlier that week?

THE COURT: 15th?

MR. BOWERS: That's fine, your Honor.

MR. LAYDEN: That works.

MR. STEPHAN: That's good.

THE COURT: Same thing. 10:00 status or argument. And then you guys work out a briefing schedule. If somebody wants to e-mail an order, if it gets to that point, I'd be happy to enter the order without a court appearance. Okay?

So if you'd indicate today for the

reasons stated on the record, and then just go from there.

Anything else we can accomplish?

MS. JENKINS: No, your Honor.

MR. STEPHAN: Thank you, Judge.

MR. LAYDEN: Thanks, your Honor.

STATE OF ILLINOIS)
)
COUNTY OF C O O K)

NOHEMI SALAZAR-PITTS, a Certified Shorthand Reporter doing business in and for the State of Illinois certifies that she reported in shorthand the proceedings of said hearing, and that the foregoing is a true and correct transcript of her shorthand notes so taken as aforesaid and contains the proceedings given at said hearing.

_____
Certified Shorthand Reporter

Exhibit F

IN THE CIRCUIT COURT OF COOK COUNTY, ILLINOIS
COUNTY DEPARTMENT, CHANCERY DIVISION

FELIPE BERNAL, individually and on behalf of others similarly situated, Plaintiff, v. ADP, LLC, Defendant.	No. 2017-CH-12364 Calendar 16 Judge David B. Atkins

MEMORANDUM OPINION AND ORDER

THIS CASE COMING TO BE HEARD on Defendant ADP, LLC's Motion to Dismiss Plaintiff's Complaint Pursuant to 735 ILCS 5/2-615, the court, having considered the briefs submitted and being fully advised in the premises,

HEREBY FINDS AND ORDERS:

Background

Plaintiff, Felipe Bernal, as an employee of Rockit Ranch Productions, Inc. ("Rockit"), was required to use biometric scanning technology to "clock-in" and "clock-out." The biometric technology was provided and serviced by Defendant ADP, LLC. Plaintiff alleges the use of his biometric identifying information during his employment with Rockit was improperly acquired, possessed, and disseminated in violation of sections 740 ILCS 14/15 (a)-(d) of the Biometric Information Privacy Act ("BIPA"). Plaintiff originally brought suit against Rockit for said violations, but he subsequently amended his Complaint to drop all allegations against Rockit and instead claim that Defendant violated BIPA. Defendant now seeks to dismiss all counts.

Standard of Review

A 2-615 motion to dismiss challenges the complaint's legal sufficiency based on facial defects.[1] The court assumes all well-pleaded facts and their reasonable inferences in the complaint as true, viewing the allegations in the light most favorable to the plaintiff.[2] As Illinois is a fact-pleading jurisdiction, "a plaintiff must allege facts sufficient to bring a claim within a legally recognized cause of action."[3] Mere conclusions of law and unsupported conclusory factual allegations are insufficient to survive a 2-615 motion to dismiss.[4] A 2-615 motion to dismiss does not raise affirmative factual defenses.[5] "A

[1] *Beacham v. Walker*, 231 Ill. 2d 51, 57 (2008).
[2] *Alpha School Bus Co. v. Wagner*, 391 Ill. App. 3d 722, 735 (2009).
[3] *City of Chicago v. Beretta U.S.A. Corp.*, 213 Ill. 2d 351, 355, (2004).
[4] *Alpha School Bus*, 391 Ill. App. 3d at 736.

motion to dismiss should be granted only if the plaintiff can prove no set of facts to support the cause of action asserted."[6]

Discussion

Count I of Plaintiff's Complaint alleges violations of four separate clauses within BIPA. The Court addresses each alleged violation separately.[7]

Applicability of § 15(b).

Plaintiff asserts that Defendant violated § 15(b), which imposes certain preconditions that private entities must comply with before they can "collect, capture, purchase, receive through trade, or otherwise obtain" an individual's biometric information. Defendant presents a compelling argument that § 15(b) should not apply to an entity like ADP, pointing out that language included by the legislature differs from the language included in the other subsections and suggests that the legislature intended for possession alone to not be enough to make an entity subject to § 15(b). Indeed, § 15(b)'s requirement that the private entity whose actions the subsection is meant to regulate must receive a "written release" from the subject of the biometric identifier or biometric information or their legally-authorized representative does suggest that the legislature did not intend for the subsection to apply to a third party entity as Defendant seems to be here.[8] Here, Defendant is not Plaintiff's employer. While Plaintiff correctly contends that BIPA can be applied outside of an employment situation, there is nothing to suggest that BIPA was intended to apply to situations wherein the parties are without any direct relationship.[9] Moreover, from the facts as they are alleged, the Court can infer that this case fits squarely within an employment context. All of Plaintiff's claims stem from Rockit's requirement that employees participate in biometric scanning technology. That Rockit obtained the technology from Defendant does not remove Plaintiff's case from existing within the context of his employment by Rockit. As Defendant notes, to read BIPA as requiring that a third party provider of the biometric timeclock technology, without any direct relationship with its customers' employees, obtain written releases

---

[5] *Borowiec v. Gateway 2000, Inc.*, 209 Ill. 2d 376, 382 (2004).

[6] *Kaiser v. Fleming*, 315 Ill. App. 3d 921, 925, (2000).

[7] In his response to Defendant's motion to dismiss, Plaintiff represents that he "voluntarily dismisses his negligence claim (Count II) against Defendant," thus rendering as moot Defendant's motion to dismiss Count II.

[8] As Defendant notes in its motion, the BIPA's definition of "written release" clearly limits its applicability, in the context of employment, to the relationship that exists between employer and employee. 740 ILCS 14/10.

[9] In *Rosenbach v. Six Flags Entm't Corp.*, 2019 IL 123186 (2019), the Supreme Court noted that the purpose of § 15(b) is to vest "in individuals and customers the right to control their biometric information without requiring notice before collection and giving them the power to say no by withholding consent." 2019 IL 123186 at ¶34. Given the Supreme Court's interpretation of § 15(b)'s purpose, there is little reason to believe that its applicability should extend beyond the point at which an individual has the right to withhold consent. Here, Plaintiff's right to withhold consent can be exercised by refusing Rockit's authority to collect his biometric information.

from said employees would be unquestionably not only inconvenient but arguably absurd.[10]

Yet, based on the pleadings, as written, the Court's decision must ultimately turn on the insufficiency of Plaintiff's Complaint as to § 15(b). Plaintiff has failed to allege facts sufficient enough for the Court to properly assess Defendant's actual involvement, relative to the biometric scanning technology, beyond the fact that Defendant supplied Rockit with the technology. In order for the Court to determine whether or not § 15(b) is applicable here, Plaintiff's Complaint must include factual allegations of what Defendant's role relative to Plaintiff's biometric information is. Most of Plaintiff's claims that are relevant to § 15(b) are aimed at what the technology Defendant provides to Rockit allegedly does. In so far that Plaintiff's claims allege particular action on Defendant's part, the allegations are conclusive in nature.[11] Therefore, Defendant's motion to dismiss, as to the portion of Count I alleging a violation of § 15(b) of BIPA is GRANTED.

Whether § 15(a) is Moot.

Plaintiff alleges a breach of § 15(a), which requires private entities in possession of biometric information to:

> "develop a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers ... when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within 3 years of the individual's last interaction with the private entity, whichever occurs first. Absent a valid warrant or subpoena issued by a court of competent jurisdiction, a private entity in possession of biometric information must comply with its established retention scheduled and destruction guidelines."

The language in § 15(a) seems to make clear that a private entity is required to comply with its established retention schedule and destruction guidelines whenever in possession of biometric information. The subsection seems to stipulate that the schedule and guidelines must be written and made available to the public. Therefore, if a private entity is in possession of biometric information, but lacks an established retention schedule and destruction guidelines, it stands to reason that said private entity could be found to be in violation of § 15(a).

Notwithstanding the requirement that a private entity in possession of biometric information have an established retention schedule and destruction guidelines, there is no explicit requirement that the schedule or guidelines exist "prior to" possession of the

---

[10] "It is a familiar rule, that a thing may be within the letter of the statute and yet not within the statute, because not within its spirit, nor within the intention of its makers." *People v. Hanna*, 207 Ill. 2d 486, 498 (2003) (citing *Croissant v. Joliet Park Dist.*, 141 Ill. 3d 449, 455 (1990) ("Statutes are to be construed in a manner that avoids absurd or unjust results")).

[11] See Plaintiff's Complaint at ¶ 3 ("Defendant ADP is capturing, storing, using, and/or disseminating the biometrics of Plaintiff ...")

biometrics information. Yet, regarding § 15(a), Plaintiff alleges that "[p]rior to taking Plaintiff's biometrics, Defendant did not make publicly available any written policy as to a biometric retention schedule and guidelines for permanently destroying the collected biometrics." While this may be true, such an allegation does not exclude the possibility that Defendant made available to the public an established schedule and guidelines when, and not before, it was in possession of Plaintiff's biometric information. Plaintiff's Complaint, as written, does not sufficiently allege an actual violation of § 15(a), and thus, fails to state a claim. Defendant's motion to dismiss, as to the portion of Count I asserting a violation of § 15(a) of BIPA is GRANTED.

Whether Plaintiff has Sufficiently Alleged a Violation of § 15(c).

Plaintiff alleges an infraction of § 15(c), which prohibits private entities from selling, leasing, trading, or otherwise profiting from an individual's biometric information.[12] Here, Plaintiff's contends that the allegations in his Complaint, "when combined with reasonable inferences that can be drawn therefrom, establish that Defendant obtains and stores the biometric information captured by its devices, which it in turn sells, leases, or otherwise makes commercially available to Plaintiff's employer for the purposes of biometric timekeeping."[13] The court disagrees. Paragraphs 11 and 26 of Plaintiff's Complaint allege that Defendant disseminates biometric information to "third parties, including vendors for timekeeping, data storage, and payroll purposes." Plaintiff's Complaint does not contain any allegation that Defendant sold, leased, traded, or otherwise profited from anyone's biometric information. Thus, since Plaintiff's Complaint only alleges facts sufficient to demonstrate that Defendant passes biometric data to third party partners for purposes other than profit, Defendant's motion to dismiss as to the portion of Count I asserting a violation of § 15(c) is GRANTED.

Whether Plaintiff has Sufficiently Alleged a Violation of § 15(d).

Defendant provides a compelling argument regarding whether § 15(d) is even applicable in this case. Namely, that Plaintiff's implication of Defendant's allowing biometric information to pass to data storage vendors and payroll services does not qualify as instances of "disclosure" or "dissemination" under BIPA, but rather should be considered a form of mere transmission. However, to the extent that Defendant's argument seems to suggest an affirmative factual defense, it would be inappropriate for the Court to entertain this line of argument on a Section 2-615 motion to dismiss.

Turning to the Complaint as pled, Plaintiff asserts a violation of § 15(d), which establishes certain preconditions with which private entities must comply before they "disclose, redisclose, or otherwise disseminate a person's or a customer's biometric … information." Only twice in Plaintiff's Complaint does he allege any such disclosure; each instance consists of a single statement that Defendant's technology "allows for and resulted in" the dissemination of Plaintiff's biometric information to third parties,

[12] See 740 ILCS 14/15(c).
[13] See Plaintiff's response to Defendant's motion to dismiss at pg. 8.

including vendors for timekeeping, data storage, and payroll purposes."[14] These allegations fall short of sufficient factual pleading, because they are void of any facts to support Plaintiff's allegation that Defendant has violated § 15(d). Suggesting that the technology Defendant created allows for the dissemination of biometric information is not an allegation of the Defendant's disseminating biometric information. Thus, Defendant's motion to dismiss, as to the portion of Count I asserting a violation of § 15(d) is GRANTED.

WHEREFORE the Court enters an order as follows:

a. Defendant ADP, LLC's motion to dismiss Plaintiff Felipe Bernal's Complaint is GRANTED, and Count I is dismissed *without prejudice*.

b. Plaintiff has until September 20, 2019 to file an amended complaint, with facts consistent with this Order.

c. This matter is set for further status to October 24, 2019 at 10:30 a.m. in courtroom 2102.

ENTERED: JUDGE DAVID B. ATKINS
AUG 23 2019
Circuit Court-1879

Judge David B. Atkins

The Court.

[14] See Plaintiff's response to Defendant's motion to dismiss at ¶¶11, 26.